BELKIN®

Servidor de consola serie OmniView®



Manual del usuario

F1DP116Sea

Introducción

Gracias por adquirir el servidor de consola serie OmniView (el servidor de consola). Este dispositivo permite a los administradores supervisar y controlar servidores, routers, conmutadores y otros dispositivos serie de un modo seguro, desde cualquier lugar de la red TCP/IP corporativa, por Internet o a través de conexiones telefónicas por módem, incluso cuando el servidor no está disponible a través de la red.

La consola para servidor ofrece lo siguiente:

- Transferencia de datos segura mediante SSH o Web/SSL
- Una interfaz de Internet segura y encriptada a través de SSL (HTTPS)
- Encriptación SSHv2, para proteger las contraseñas de acceso a los servidores de los hackers
- Compatible con todos los clientes SSH conocidos
- Acceso seguro desde cualquier navegador con tecnología Java
- Las conexiones a los puertos serie de la consola mediante cables CAT5 estándar, eliminan las molestias del cableado personalizado

Contenido del paquete

1 x Consola OmniView® para servidores serie

1 x Cablede alimentación de CA

5 x Adaptadores de serie a RJ45 (5 piezas)

1 x Adaptador serie para el puerto de la consola local

1 x Cable CAT5 RJ45-RJ45 de 1,8m

1 x Guía de instalación rápida

1 x CD del manual de usuario

1 x Soportes y tornillos para montaje en bastidor

1 x Kit de plataforma

Características de la consola para servidor

- **Control en banda y fuera de banda**
  Las soluciones para el control del puerto de la consola ofrecen un acceso remoto, fiable y seguro, a los puertos serie de la consola mediante redes en banda y opciones de conectividad fuera de banda, como acceso al terminal serie o conexión telefónica por módem.
- **Controle dispositivos/servidores en red de manera remota, centralizada y segura**
  Las fiables soluciones para el control del puerto de la consola le permiten encriptar información delicada utilizando protocolos probados como SSH/v2,SSL.
- **Control de diversos dispositivos**
  La simple emulación del terminal VT-100 o ASCII no es suficiente para controlar esta amplia gama de tipos de dispositivos. Los centros de datos actuales contienen una amplias mezcla de servidores UNIX®, Linux®, RISC, mainframe, y Windows®, así como otros dispositivos controlados mediante puerto serie como routers, pasarelas, firewalls, dispositivos PBX, UPS, SAN y NAS, y regletas de alimentación inteligentes.
- **Supervisión y aviso proactivos para asistir en el diagnóstico de sistema**
  Las aplicaciones, e incluso los sistemas operativos, envían mensajes a la consola de sistema. Los mensajes contienen información sobre errores o situaciones críticas que a menudo preceden a un fallo en el sistema. A diferencia de los servidores terminal, los servidores de puertos de consola almacenan estos mensajes en tiempo real y permiten a los administradores buscar y encontrar estos datos en otro momento. También mandan un correo electrónico de manera automática al administrador TI para avisarlo de la situación crítica.
- **Controlador de alimentación remoto y seguro**
  A través del puerto serie, este dispositivo actúa como control principal de las regletas de alimentación. Puede controlar múltiples regletas de alimentación (hasta 15).
- **Proporciona la función de serie a serie**
  Esto permite al dispositivo incorporar un convertidor de terminal para proporcionar puertos VGA y de teclado de forma local, o conectar los puertos VGA/de teclado a un conmutador KVM para consolidar la administración.
- **Acceso a la lista de puertos para usuarios**
  Gracias a la lista de control de acceso (ACL) de la administración de cuentas de usuario, todos los usuarios excepto **los que tengan cuenta** de administrador, tienen autorización para un conjunto de puertos serie. Los usuarios pueden acceder y realizar cambios en la configuración de estos puertos autorizados que han sido asignados por **una cuenta de** administrador.

Requisitos del equipo

- Kit de conexión universal (incluido)
- Cable RJ45-RJ45 CAT5 (incluido)

Requisitos del sistema

Navegador de Internet

Explorador		
Sistema operativo	Microsoft Internet Explorer versión 6.0 SP1 o superior	Firefox versión 2.0 o superior
Windows 2000 SP2	Sí	Sí
Windows 2003 Server	Sí	Sí
Windows XP	Sí	Sí
Windows Vista	Sí	Sí
Red Hat Linux 3 y 4	No	Sí
Sun Solaris 9 y 10	No	Sí
Novell SUSE Linux 9 y 10	No	Sí
Fedora Core 4 y 5	No	Sí
Mac OS X 10.4+	No	Sí

Conexión Java

La interfaz de Internet del servidor de consola requiere la instalación de JRE (Java Runtime Environment) v6.0 o superior Puede conseguir el último software Java de la página de Internet: http://www.java.com/en/download/manual.jsp.

Diagramas de los indicadores de la unidad

Panel frontal/trasero

Fig. 1 Vista frontal

LED de vínculo

tación

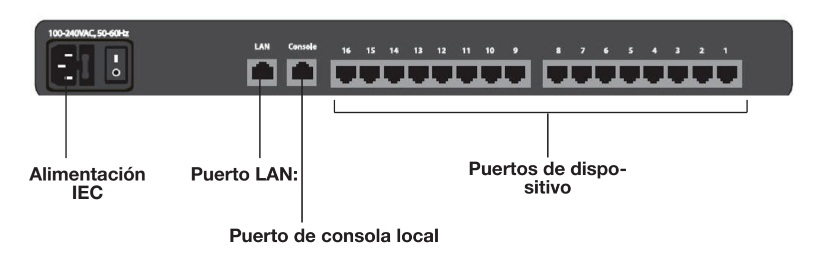
LED de alimen-

LED indicador de listo

LEDs de puerto

Botón de reinicio

Fig. 2 Vista trasera



Indicadores LED, botones y conectores

LED	Indicador
Alimentación	**Rojo:** indicador de alimentación *ENCENDIDO: la alimentación está conectada*
Vínculo	**Vínculo Ethernet/Act/10/100Mbps:** **Naranja:** Conexión Ethernet 10BaseT establecida **Verde:** Conexión Ethernet 100BaseT establecida *Intermitente: actividad de datos* *ENCENDIDO: sin actividad de datos y vínculo conectado*
Listo	**Verde:** intermitente con un intervalo de un segundo cuando el sistema está listo

- **botón de** REINICIO. Pulse y suelte el botón rápidamente para reiniciar el servidor de consola. Pulse y mantenga pulsado el botón de reinicio durante más de cinco segundos para volver a los ajustes de configuración por defecto.
- **conector** ETHERNET RJ45: interfaz Ethernet
- **conector de**CONSOLA RJ45: interfaz de consola local RS232
- **Otros** conectores RJ45: Puertos serie

Especificaciones

Característica	Especificación
General	**Indicadores LED** Alimentación (rojo) Listo (verde, parpadeo normal), Link/Act/10/100Mbps (Ethernet naranja: 10Mbps, verde: 100Mbps)
	Actividad (azul para cada puerto serie)
	Pulse el botón para reiniciar o para volver a los valores por defecto
	RTC ("real-time clock", reloj a tiempo real)
Interfaz serie	16 puertos (F1DP116S)
	Modo puerto serie (RS232)
	Conector serie (RJ45)
	Tasa de baudios (de 300 a 115200)
	Control del flujo (Ninguno, RTS/CTS, Xon/Xoff)
Interfaz LAN	Conector RJ45
	IEEE 802.3 - 10/100BaseT
	Auto-detección, modos full/half duplex seleccionables
Función de puerto	**Modos de funcionamiento**
	Servidor de consola
	Servidor terminal
	Módem por línea telefónica
	Puerto serie a serie (sólo en el puerto 16)
Protocolos	TCP, UDP, IP, ARP, ICMP, HTTP/HTTPS, Telnet, DHCP/BOOTP, PPP,
	SMTP, DNS, NTP
	DNS dinámico
Función relativa al protocolo	Tiempo de inactividad TCP (TCP keep-alive time)
	Tiempo de inactividad del puerto serie
	Supervisión del puerto
Seguridad	Acceso protegido por contraseña
	Filtración IP
	SSHv2
	HTTPS/SSL
Autenticación	Base de datos local del usuario
	PAP/CHAP (para módem con conexión telefónica)
	RADIUS
Gestión	Consola local (línea comando o menú)
	SSH, telnet
	Páginas de Internet (HTTP/HTTPS)
	Actualización del firmware a través de la interfaz de Internet
	Acceso y almacenamiento de puertos
	Pantalla completa de estado del sistema
Alimentación y entorno	Entrada de CA (100 ~ 240 V AC, 50 ~ 60 Hz)
	Temperatura de funcionamiento: de -10 a 80° C
	Temperatura de almacenamiento: de -20 a 85° C
	Humedad: 0 – 90% (sin condensación)
Certificaciones	CE, FCC
	UL
Características mecánicas	1U de montaje en bastidor de19˝
	Dimensiones (cm) 43,2 x 18,0 x 4,2

Nota: Las especificaciones pueden ser objeto de modificación sin previo aviso.

Dónde colocar el servidor de consola:
La carcasa del servidor de consola está diseñada para colocarse de forma autónoma en el escritorio o para montarse en bastidor. El servidor de consola puede montarse en un bastidor estándar de 19 pulgadas para servidores, utilizando los soportes para montaje en bastidor y los tornillos que se incluyen.

Tenga en cuenta los siguientes aspectos a la hora de decidir dónde colocar el servidor de consola:

- la ubicación de sus dispositivos de destino con respecto a la consola
- la longitud de los cables que utiliza para conectar los dispositivos a la consola
- la fuente de alimentación: debe conectarse sólo a la fuente de alimentación especificada en la unidad. Cuando se instalen varios componentes eléctricos en un bastidor, asegúrese de que las tasas de alimentación totales no exceden la capacidad del circuito.

Requisitos de longitud de cables (para CAT5)
Las señales de datos binarios serie (RS232) se transfieren correctamente a distancias de hasta 15 m Cuando se supera esa longitud, aumenta la posibilidad de degradación de la señal. Por esta razón, Belkin recomienda que la longitud del cable UTP CAT5 que conecta la consola y los servidores no supere los 15 m

Cables y adaptadores
Belkin recomienda encarecidamente la utilización de cables de red Belkin Categoría 5e, FastCAT5e o Categoría 6 para su servidor de consola, para asegurar la integridad de la señal.

Cables de red UTP de Belkin:

A3L791-XX-YYY (CAT5e)

A3L850-XX-YYY (FastCAT™ 5e)

A3L980-XX-YYY (CAT6)

Véase el anexo B de la página 54 para consultar la guía de conexiones.

Adaptador serie de Belkin

F1D120ea (RJ45F – DB9F DTE)

F1D121ea (RJ45F – DB25F DTE)

F1D122ea (RJ45F – DB25M DCE)

F1D123ea (RJ45F – DB25M DTE)

F1D124ea (RJ45F – RJ45M CISCO)

F1D120ea-8PK (pack de 8 F1D120ea)

F1D120ea-8PK (pack de 8 F1D120ea)

Véase el anexo A de la página 51 para obtener dibujos detallados de cada adaptador serie.

Instalación en el escritorio o montaje en bastidor

La consola de servidor puede colocarse sobre escritorios o montarse en bastidores de 1U de 19 pulgadas.

Nota: Antes de comenzar, localice la dirección MAC y el número de serie en la parte trasera del servidor de consola. Puede necesitar estos números más adelante durante el proceso de instalación, por lo que se recomienda que los anote antes de montar el servidor de consola en el bastidor.

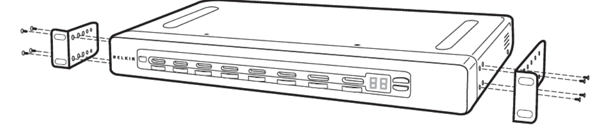
Dirección MAC	Número de serie:

El servidor de consola incluye soportes de montaje ajustables, para instalarla en un bastidor de 19 pulgadas. Los soportes de montaje admiten tres posiciones de ajuste que le permitirán colocar la parte frontal del servidor de consola a la altura de los carriles, o dejar que el servidor de consola sobresalga del bastidor. Siga estos sencillos pasos para conseguir la posición que prefiera.

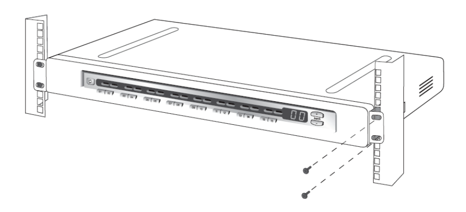
Montaje en bastidor

1. Determine cuánto debe sobresalir el servidor de consola del bastidor. Seleccione los orificios y el tipo de montaje que desea llevar a cabo.

2. Fije el soporte al lateral del servidor de consola utilizando los tornillos Phillips incluidos. (Consulte el siguiente diagrama).



3. Monte el servidor de consola en los rieles del bastidor y fíjela con los tornillos. (Consulte el siguiente diagrama).



Ahora, su servidor de consola está montada sólidamente en el bastidor y lista para conectar a sus dispositivos finales.

Conectar los dispositivos de destino a la consola para servidor

1. Desconecte de la fuente de alimentación el(los) dispositivo(s) que se conectarán a su servidor de consola.
2. Conecte el cable Ethernet con el puerto con la indicación LAN.
3. Localice el cable de alimentación incluido y conecte el extremo apropiado en el conector de alimentación de la parte trasera del servidor de consola. Introduzca el otro extremo en una toma de CA de la pared.

Nota: El proceso de inicialización del servidor de consola puede tardar hasta 100 segundos en completarse.

4. Escoja un puerto numerado disponible de la parte posterior del servidor de consola. Conecte uno de los extremos del cable de red UTP (4 pares. hasta 15 metros) al puerto seleccionado y conecte el otro extremo en el dispositivo de destino. Puede que necesite añadir el adaptador apropiado para realizar la conexión con el dispositivo de destino. Por favor, consulte el anexo A de la página 51 de este manual para obtener más detalles.
5. Repita este procedimiento para todos los dispositivos de destino. (Consulte el siguiente diagrama).

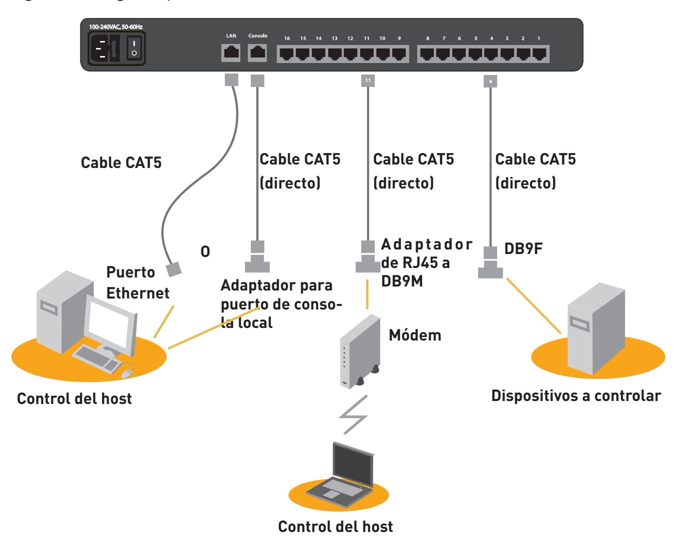


Fig. 3 Instalación de las conexiones por cable—Este diagrama muestra ejemplos de conexiones por cable para diferentes interfaces.

Antes de poder conectarse a un dispositivo de destino deberá configurar los ajustes de red. El servidor de consola ofrece dos métodos para ajustar la red: a través de la interfaz del explorador de Internet o a través del puerto de la consola local.

El servidor de consola ofrece soporte tanto para el protocolo de configuración de host dinámico (DHCP) como para las direcciones IP estáticas. Belkin recomienda reservar una dirección IP para el servidor de consola que se mantenga estática mientras esté conectado a la red.

Interfaz del explorador de Internet

La interfaz de Internet proporciona una manera sencilla de configurar el servidor de consola. El administrador puede configurar todas las características a través de Internet.

Ajustes iniciales

La siguiente sección proporciona instrucciones para ajustar la dirección IP del servidor de consola serie OmniView.

Paso 1 Identificación de la dirección IP

Una vez que su servidor de consola se haya conectado a su red y se haya encendido, un protocolo de configuración de host dinámico (DHCP) de su red asignará automáticamente al servidor de consola una dirección IP, dirección de puerta de enlace y una máscara de subred.

Para identificar la dirección IP en su red, utilice la dirección MAC ubicada en la parte posterior del servidor de consola. Si no encuentra servidor DHCP en su red, el servidor de consola se iniciará con la siguiente dirección IP estática: 192.168.2.156.

Si quiere conectar más de un servidor de consola a la misma red y no existe servidor DHCP disponible, conecte cada servidor de consola a su red de uno en uno y cambie la dirección IP estática de cada unidad antes de conectar la siguiente unidad.

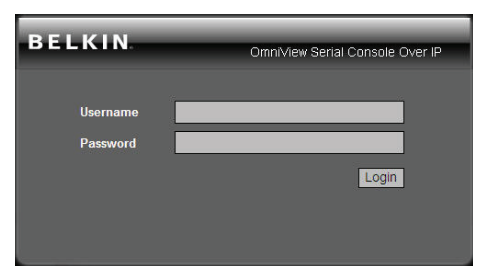
Nota: Si posteriormente hay un servidor DHCP disponible en su red, el servidor de consola adoptará la nueva dirección IP del servidor DHCP. Para conservar la dirección IP estática original, necesitará desactivar el DHCP (consulte la página 18).

Paso 2 Acceso a la interfaz de Internet

Tras identificar la dirección IP de su dispositivo, abra su explorador de Internet. Puede encontrar una lista de exploradores compatibles en la página 3.

Escriba la dirección IP del servidor de consola en el campo de la dirección del navegador, utilizando este formato: http://XXX.XXX.XXX.XXX (ejemplo: http://76.255.43.173). Aparecerá la pantalla de acceso (véase la página siguiente). Guarde la página en sus favoritos para poder consultarla fácilmente.

Nota: Se utiliza HTTPS para la comunicación mediante un mecanismo de encriptación SSL (Secure Socket Layer). La primera vez que se conecte a la página de configuración HTTPS del servidor de consola, pueden aparecer dos advertencias de seguridad del navegador. Haga clic en "Sí" (Yes) en ambas advertencias.



Página de acceso

Escriba el siguiente nombre de usuario y contraseña predeterminados (respetando mayúsculas y minúsculas):

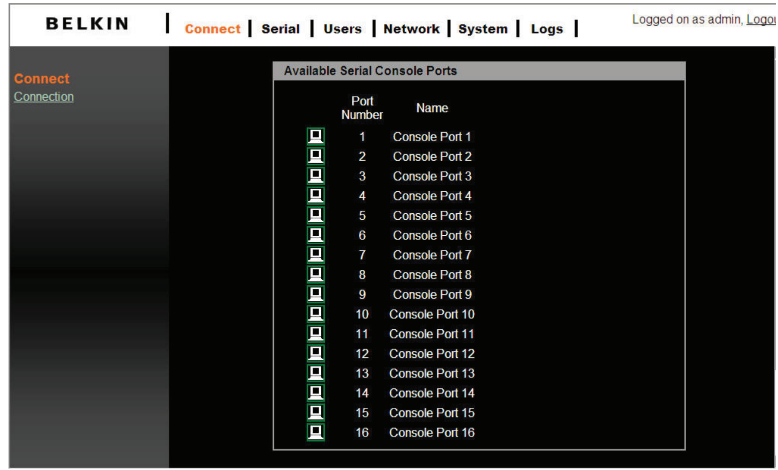
Nombre de usuario	Contraseña
admin	admin

Hay dos niveles de privilegio de acceso:

Nombre de usuario	Contraseña predeterminada	Privilegios de acceso
admin	admin	Acceso completo
(definición de usuario)	(definición de usuario)	Puede acceder solamente a "Puerto serie" y a "Estado del sistema"

El administrador puede añadir o eliminar un usuario fácilmente mediante las páginas de Internet del sistema de administración.

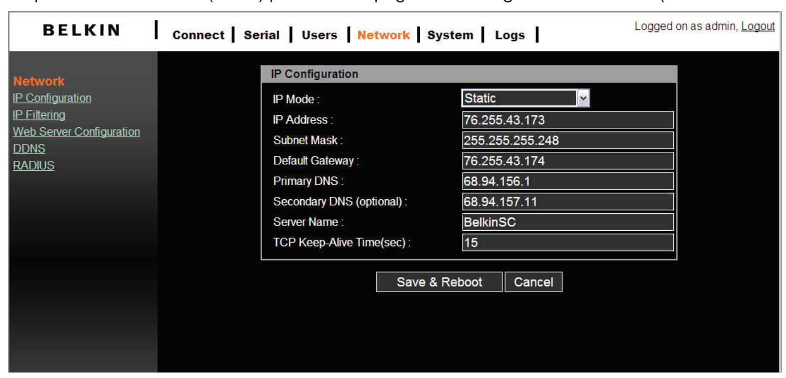
Haga clic [Nombre de acceso] La interfaz de Internet se abrirá en la página de conexión ("Connect") (véase más abajo).



Página principal de conexión

Paso 3 Configuración de la red

Clique sobre "Network" (redes) para abrir la página de configuración de la red (véase más abajo).



Página de configuración de la red

Aquí puede asignar una dirección IP estática y otros ajustes de red.

Clique en "Save & Reboot" (guardar y reiniciar) para guardar todos los ajustes de configuración de red.

Nota: Si el usuario permite que el navegador agote su tiempo máximo de detención durante más de **30 minutos**, la sesión de acceso agotará su tiempo y se cerrará.

Cómo asignar una IP desde el puerto de consola VT-100 (Console, Telnet, SSH)

El servidor de consola también ofrece una interfaz de línea para comandos guiada por un menú de fácil manejo. Puede simplemente conectar un terminal VT-100 al puerto de la consola local para acceder al servidor de consola. Esto es útil cuando no conoce los ajustes de configuración del servidor de consola y no puede acceder a él. A través del puerto de la consola local puede visualizar o cambiar los ajustes (dirección IP, máscara de subred, etc.).

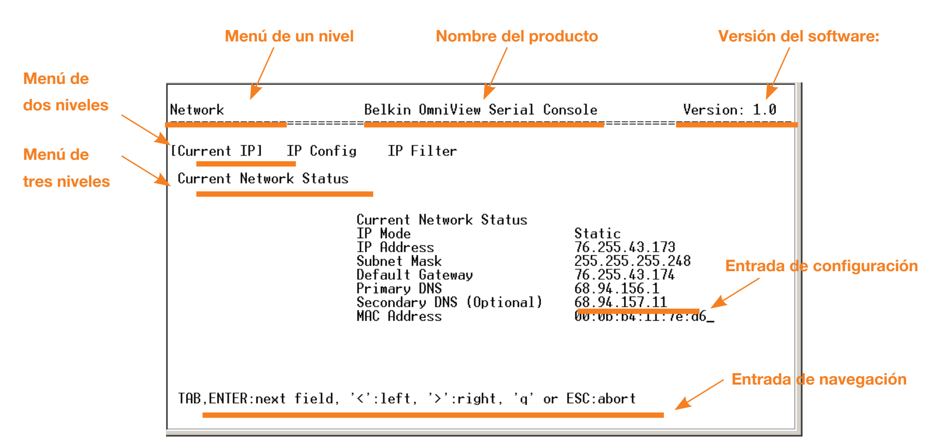
1. Conecte el puerto de la consola, situado en el panel posterior, al puerto serie del host del PC mediante un cable CAT5 y el adaptador para puerto de la consola local RJ45/DB9F, incluido en el paquete del servidor de consola de Belkin.
2. Configure un programa de emulación de terminal, como HyperTerminal, siguiendo los parámetros siguientes:
    - Tasa de baudios = 115200
    - Bits de datos = 8
    - Bits de parada = 1
    - Paridad = ninguna
    - Control de flujo = ninguno

```
        +--------------------------------------------------------------+
        |                 Belkin OmniView Serial Console               |
        |             Copyright (c) 2007, All Rights Reserved          |
        +--------------------------------------------------------------+
        |                             Log In                           |
        +--------------------------------------------------------------+

username : _
```

Nota: Los nombres de usuario y las contraseñas son los mismos que se han configurado a través de la interfaz de Internet. Por defecto son “admin/admin”.

La figura siguiente muestra la estructura de la interfaz.




```
Main                      Belkin OmniView Serial Console          Version: 1.0
================================================================================

[Network]   System    S-to-S

 Current IP    IP Config    IP Filter




 ENTER:select, TAB:next, '<':left, '>':right, 'q' or ESC:previous menu
```

El diseño del menú

Red > Config IP

La página de la izquierda muestra los elementos de configuración IP.

1. Para **modo IP** — Puede pulsar la barra ESPACIADORA para seleccionar modo Estático o DHCP.
2. Para **dirección IP, máscara de subred, pasarela por defecto, DNS primario y DSN secundario** — Puede cambiar estos ajustes de red.
3. Tras cambiar los ajustes y pulsar intro, el servidor de consola le pedirá que confirme la selección clicando sobre Sí o NO. Si hace click sobre SÍ, el servidor de consola se reiniciará y guardará los ajustes en la memoria flash.

Red > IP actual

Para mostrar los ajustes de red actuales.

Red > Filtro IP

Para activar/desactivar la función de filtro IP.

Sistema > Reinicio

Para reiniciar el servidor de consola

Sistema > Restablecer valores predeterminados

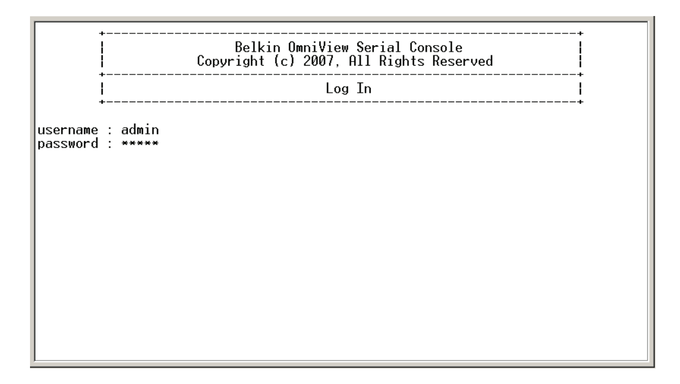
Para restablecer los ajustes de fábrica predeterminados.
Nota: Sólo el usuario **admin** tiene el privilegio de utilizar esta función.

Sistema > Estado

Para ver el estado del sistema

S a S > Seleccionar puerto de serie a serie

Para activar la conexión de serie a serie mediante el puerto 16. Consulte la sección "función de serie a serie" de la página 34 para obtener más detalles.



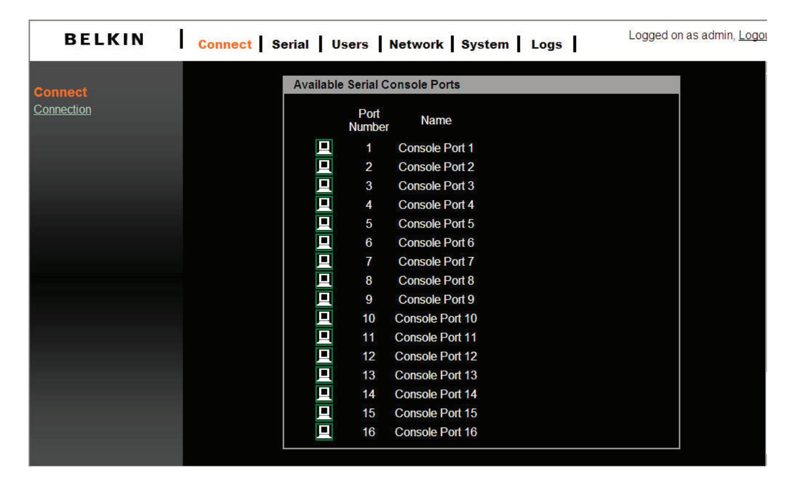
Nota:
Sólo el usuario **admin** tiene el privilegio de acceder al VT-100. Todos los demás usuarios no están autorizados a configurar con VT-100.

Interfaz de gestión del explorador de Internet

El servidor de consola es compatible tanto con el protocolo HTTP como con el HTTPS (HTTP a través de SSL). Los usuarios deben autentificarse accediendo al sistema con un nombre de usuario y contraseña seguros.

Para acceder a las páginas de gestión en Internet del servidor para consola, introduzca las direcciones IP de la unidad o un nombre de host determinable en el campo de búsqueda / URL del explorador de Internet. Esto le llevará directamente a la pantalla de acceso.

La figura de la página siguiente muestra la página de inicio de la interfaz de gestión en Internet. Una barra de menú se muestra en la parte superior de la página. El submenú se mostrará en la parte izquierda de la pantalla y le permitirá modificar los parámetros de ajuste necesarios para el elemento seleccionado en el menú superior.

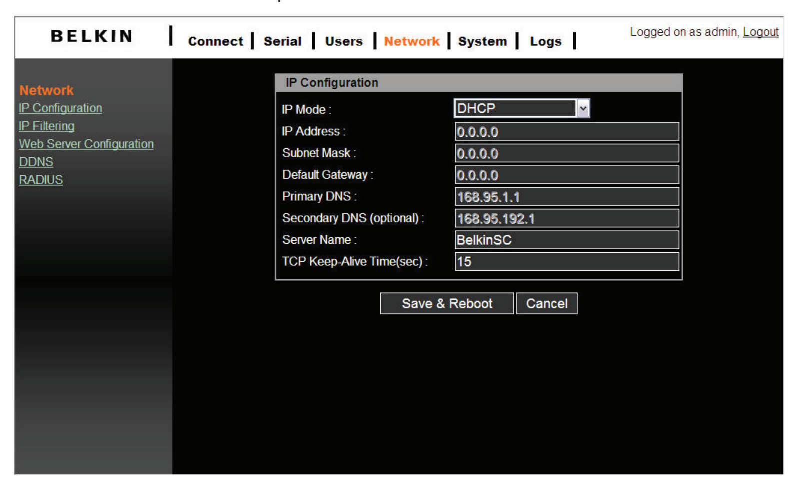


Donde esté disponible, la página permitirá a los usuarios aplicar o cancelar las acciones. Para aplicar los cambios, seleccione "Aplicar" y los nuevos valores se aplicarán a la configuración. Si no quiere guardar los nuevos valores, simplemente clique sobre "Cancelar" y todos los cambios realizados se eliminarán y se restablecerán los valores previos.

Puede configurar los ajustes de red IP a través del VT-100 o de la interfaz de Internet. Esta sección describe la configuración a través de la interfaz de Internet.

Configuración IP

El servidor de consola requiere una dirección IP válida para funcionar en el entorno de red del usuario. Si la dirección IP no es fácilmente accesible, contacte con el administrador para obtener una dirección IP válida para el servidor de consola.



Hay dos tipos de asignación IP que puede escoger:

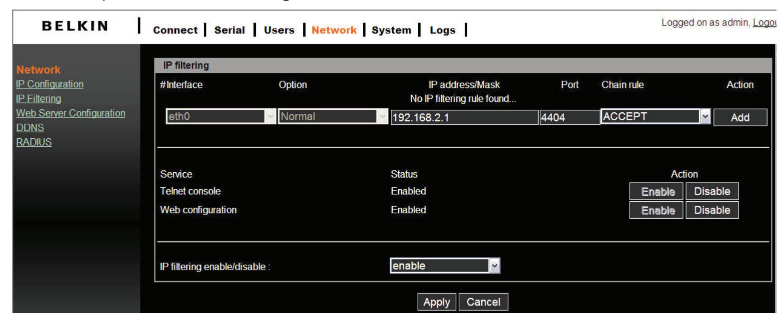
- IP estática
- DHCP Dynamic Host Configuration Protocolos (Protocolo de configuración de host dinámico).

La unidad envía con el DHCP configurado por defecto. Si no encuentra servidor DHCP en su red, el servidor de consola se iniciará con la siguiente dirección IP estática: 192.168.2.156.

El nuevo ajuste de configuración IP puede guardarse haciendo click en "Guardar y reiniciar".

Filtración IP

La función de filtración IP previene el acceso de los hosts no autorizados al servidor de consola especificando ciertas reglas.



La dirección IP/máscara especifica el alcance del host introduciendo la dirección IP básica del host seguida de "/" y la máscara de subred (es necesario utilizar "/" entre la dirección IP y la máscara de subred). Las direcciones IP del host se filtran en base a la regla definida.

La tabla siguiente proporciona ejemplos de ajustes de la dirección IP/máscara.

Alcance del host especificado	Dirección IP básica del host	Máscara de subred
Cualquier host	0.0.0.0	0.0.0.0
192.168.2.120	192.168.2.120	255.255.255.255
192.168.2.1 ~ 192.168.2.254	192.168.2.0	255.255.255.0
192.168.0.1 ~ 192.168.255.254	192.168.0.0	255.255.0.0
192.168.2.1 ~ 192.168.1.126	192.168.2.0	255.255.255.128

El "puerto" es un puerto o una serie de puertos del servidor de consola a los que los hosts intentan acceder.

Regla en cadena

La regla en cadena determina si los hosts tienen el acceso permitido o no. Puede ser uno de estos dos valores.

- **ACEPTAR:** acceso permitido
- **ELIMINAR:** acceso permitido

Cuando el servidor de consola recibe un paquete TCP procesa el paquete con la regla en cadena que se muestra a continuación. El orden del proceso es importante, el paquete introducirá la regla en cadena 1 primero. Si encuentra la regla tomará alguna acción, sino, pasará a la regla en cadena 2.

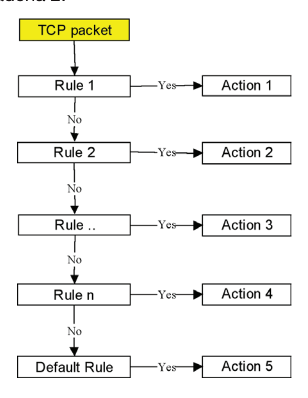
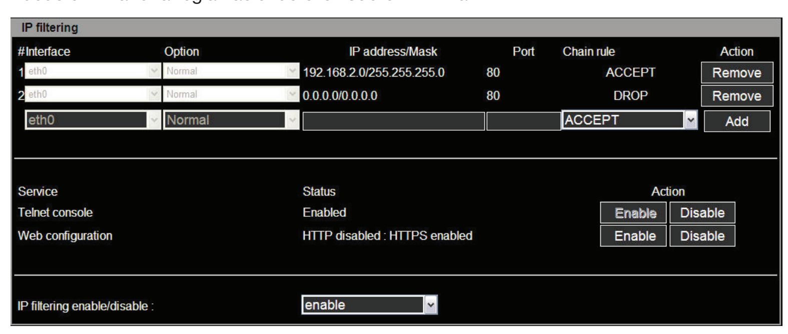


Fig. 4 Regla en cadena del filtro IP

Puede añadir una nueva filtración IP ajustando las propiedades en la primera línea disponible. Una vez se ha introducido la regla, haga click en "Añadir" para guardar la acción. Puede eliminar una regla haciendo click sobre "Eliminar".



En el ejemplo de arriba las normas se aplican en el orden siguiente:

#1. Los hosts que dependen de la subred 192.168.2.x tienen el acceso permitido al servidor de consola (mediante el puerto http 80).

#2. No todos los hosts tienen el acceso permitido al servidor de consola (mediante el puerto http 80).

Tras la aplicación de estas reglas, sólo los hosts que pertenezcan a la subred 192.168.2 x tienen el acceso permitido al servidor de consola (mediante el puerto http 80)

Además de la regla en cadena del filtro IP mencionada anteriormente, la interfaz de Internet siempre proporciona una forma conveniente de activar/desactivar telnet (puerto 23) o la configuración de Internet del puerto (puerto 80/443). Estos servicios son principalmente para la configuración del servidor de consola. Clicar sobre "Activar/Desactivar" en el campo "Acción" le ayudará a añadir/modificar la regla en cadena rápidamente, sin las molestias de editar la regla de forma manual.

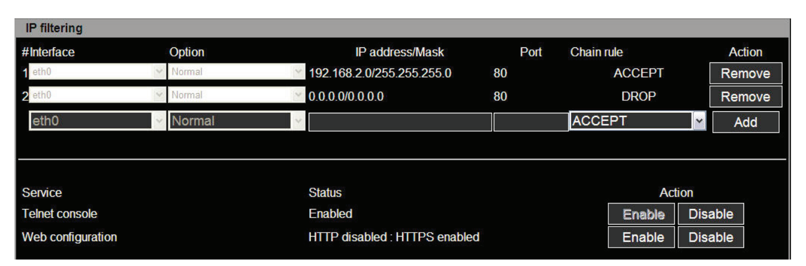
> **Nota:**
> Con el fin de conseguir una mejor alineación del texto, es preferible utilizar un cliente telnet VT-100 para alinear la salida del texto. PuTTY es uno de los clientes telnet recomendados que ofrecen mejor alineación de texto UI. Puede descargarse de
>
> http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Configuración del servidor de Internet

El servidor de Internet del servidor de consola es compatible simultáneamente tanto con el protocolo HTTP como con el HTTPS (HTTP a través de SSL).
Puede escoger el método de autenticación del usuario para el acceso a Internet. Actualmente, el servidor de consola proporciona métodos de autenticación locales y RADIUS.

Local

El servidor de consola, por defecto, indica la base de datos local para la autenticación del usuario en el acceso al servidor de Internet.



RADIUS y local

El servidor de consola hace primero referencia al servidor RADIUS para la autenticación de cuentas de usuario. Si no se encuentra la cuenta de usuario o el servidor RADIUS está desconectado, el servidor de consola busca en su propia base de datos local para encontrar la cuenta de usuario. La unidad no permitirá el acceso a un usuario si ni el servidor RADIUS ni la base de datos local encuentran la cuenta de usuario. El ajuste de servidor RADIUS se puede configurar mediante la página de configuración del servidor RADIUS. Consulte la página 24.

DNS dinámico

Si un usuario conecta el servidor de consola a una línea DSL o utiliza una configuración DHCP para obtener una dirección IP dinámica de la red, la dirección IP puede cambiar. Esto puede hacer que sea difícil saber si una dirección IP ha cambiado o cuál es la nueva dirección IP.

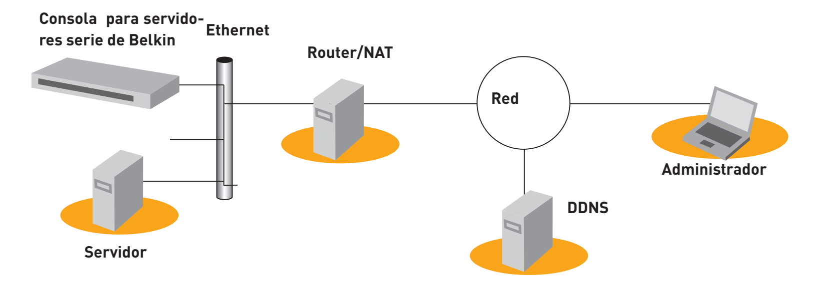
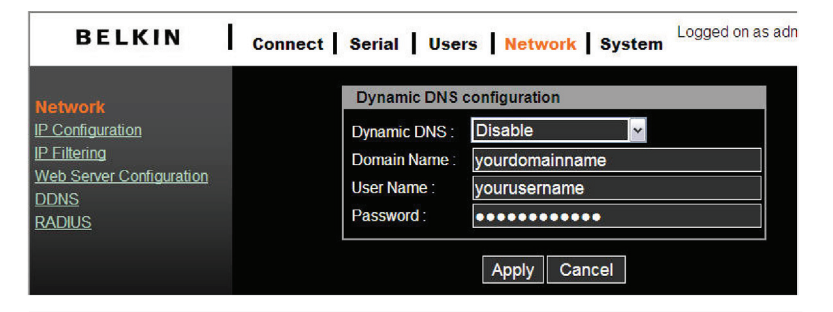


Fig. 5 DNS dinámico

El servicio DSN dinámico lo proporcionan varios PSI y organizaciones para tratar el problema anteriormente mencionado. Utilizando un DSN dinámico, puede acceder al servidor de consola mediante el nombre de host registrado en el servidor DNS dinámico, a pesar de que la dirección IP cambie. Por defecto, el servidor de consola sólo es compatible con el servicio DSN dinámico ofrecido por Dynamic DSN Services, LLC (www.dyndns.org).

^Para utilizar el servicio DNS dinámico proporcionado por Dynamic DNS Network Services, debe configurar una cuenta en el NIC (Centro de información de red) de Miembros: http://members.dyndns.org). Puede entonces añadir un enlace para el host DNS dinámico nuevo tras acceder al NIC de miembros de Dynamic Network Services.

Tras activar el servicio DSN dinámico en el menú de configuración del DSN dinámico, tiene que entrar el nombre registrado del dominio, el nombre de usuario y la contraseña. Tras aplicar el cambio de configuración podrá acceder al servidor de consola utilizando el nombre del dominio. El DSN ("Domain Name Systems", Sistemas de nombres de dominio) es el servicio de Internet que traduce los nombres de dominio en direcciones IP.



Nota:
El campo nombre de dominio requiere un nombre de dominio cualificado (FQDN) en lugar de un nombre de host registrado.

RADIUS

La autenticación es el proceso para identificar un individuo, normalmente basándose en un nombre de usuario y una contraseña. El servidor de consola es compatible con diversas opciones de autenticación, como "Local" y "RADIUS", para autenticar a los usuarios que acceden al puerto serie. Cuando la autenticación está configurada como "Local", la unidad utilizará su propia lista de usuarios para identificar un usuario. Si está configurado de otra manera, el servidor de consola pedirá autenticación a servidores de autenticación externos (p. ej. RADIUS). La figura siguiente muestra de forma conceptual el proceso de autenticación del usuario utilizando un servidor de autenticación externo.

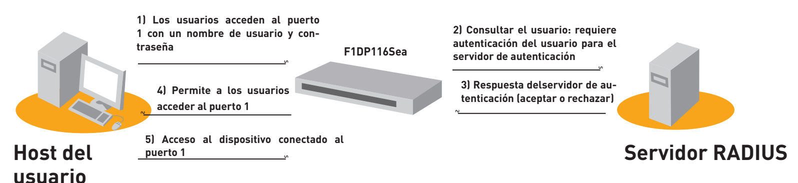
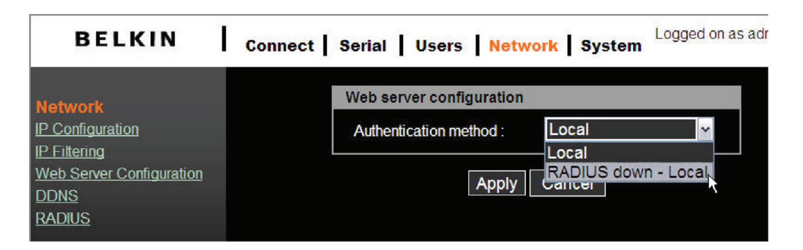
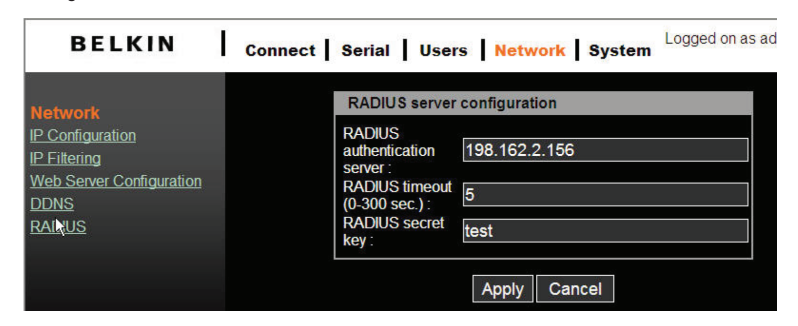


Fig. 6 RADIUS



sección
1
2
3
4
5
6
7
8

Configuración del servidor RADIUS



> **Nota**:
> Con el fin de hacer efectivo el servicio RADIUS, debe instalarse un servidor RADIUS

HTTPS/SSL

El servidor de consola es compatible simultáneamente tanto con el servicio HTTP como con el HTTPS (HTTP a través de SSL). Puede activar o desactivar la función de seguridad de cada puerto de forma individual.

HTTPS proporciona una interfaz de Internet segura y encriptada a través de SSL (secure sockets layer).

Para el protocolo HTTPS deben seguirse los pasos siguientes:

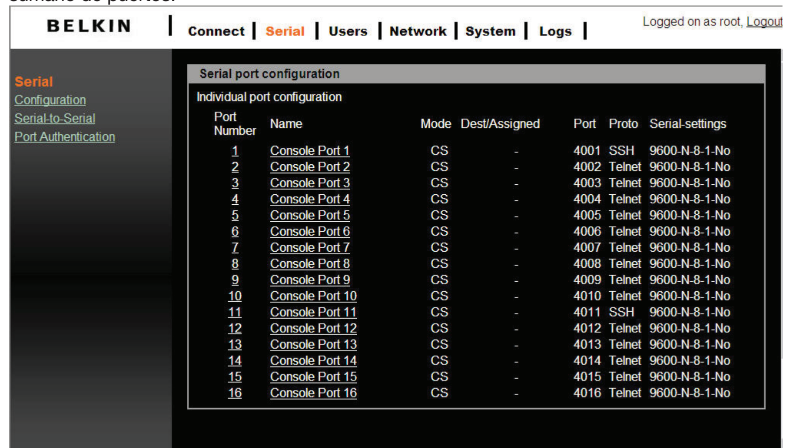
1. Cambiar el URL de “http://xxx.xxx.xxx/” a “https://xxx.xxx.xxx/”.



Haga doble click sobre el símbolo de bloqueo para mostrar la información certificada detalladamente.

Configuración

Debajo del encabezado del menú "Serie", clique sobre "Configuración" para ver la lista de sumario de puertos.

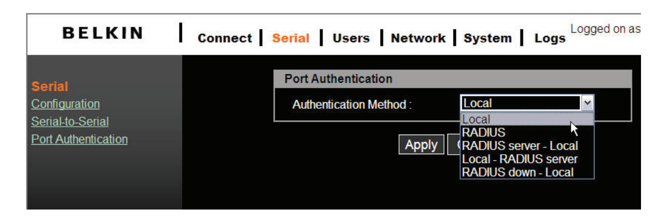


Tenga en cuenta que si el "Puerto serie"está deshabilitado, el panel de "Configuración del puerto serie" mostrará el puerto en gris oscuro. Un puerto serie activado se mostrará en en negrita y en blanco.

Autenticación del puerto

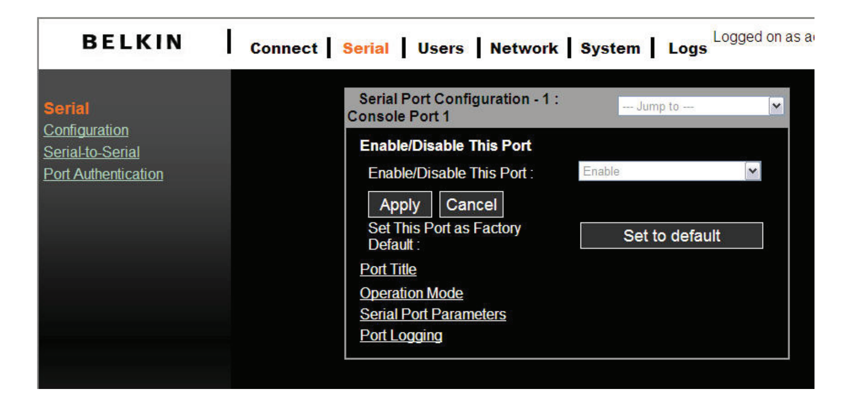
La autenticación es el proceso para identificar un individuo, normalmente basándose en un nombre de usuario y una contraseña. El servidor de consola es compatible con diversas opciones de autenticación, como "Local" y "RADIUS", para autenticar a los usuarios que acceden al puerto serie. Consulte la página 23.

Cuando la autenticación está configurada como "Local", el servidor de consola utilizará su propia lista de usuarios para identificar un usuario. Si está configurado para RADIUS, la unidad pedirá autenticación a servidores de autenticación externos (p. ej. RADIUS). La figura siguiente ilustra de forma conceptual el proceso de autenticación del usuario utilizando un servidor de autenticación externo.



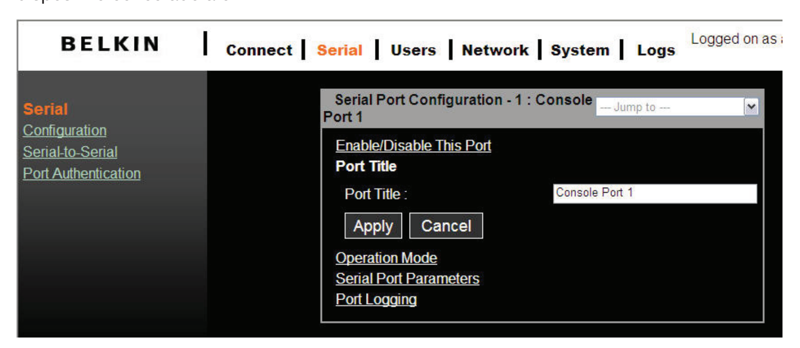
Activar / Desactivar puerto

Cada puerto serie puede activarse o desactivarse de forma individual. Un usuario no puede acceder a un puerto serie desactivado. Los usuarios pueden recuperar los ajustes por defecto del puerto serie haciendo click sobre el botón "Configuración por defecto".



Título del puerto

Los usuarios pueden introducir información descriptiva para cada puerto basándose en el dispositivo conectado a él.



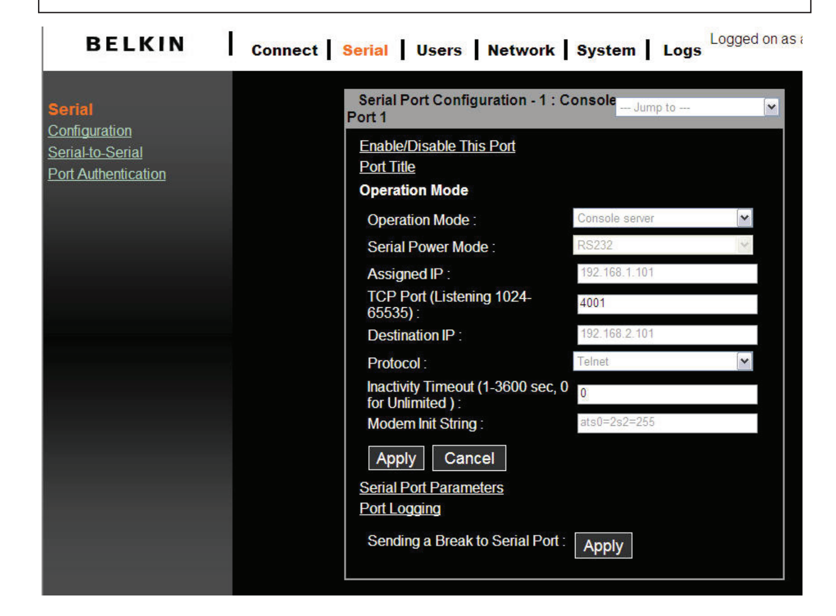
Se puede utilizar el acceso directo “--Jump to--” de la esquina superior derecha para seleccionar y configurar otro puerto.

Modos de funcionamiento

El servidor de consola proporciona cuatro tipos de modos de funcionamiento. Están descritos más abajo.

Nota:

- El último puerto (p. ej. el puerto 16) también puede utilizarse como “External ESP (Entry Serial Port, Puerto serie de entrada)” en el modo de funcionamiento “Serial-to-Serial” (serie a serie). Refiérase a la sección “Serial-to-Serial Function” (Función serie a serie) para obtener detalles.



Modo servidor de consola

Configurar un puerto serie como servidor de consola crea un socket TCP en la unidad que escucha a una conexión de cliente SSH o telnet. Cuando se conecta al socket TCP, tienen acceso al dispositivo conectado al puerto serie como si el dispositivo estuviera directamente conectado a la red. Pueden realizarse transferencias de datos pueden entre el dispositivo y el programa del cliente SSH/telnet. El RawTCP también es compatible con el modo de servidor de consola.

Los siguientes parámetros pueden configurarse en el modo de servidor de consola.

Número del puerto de escucha TCP
También puede acceder a un puerto serie mediante la dirección IP del servidor de consola y el puerto de escucha TCP.

Si la dirección IP del servidor de consola y el puerto serie están asignados como 192.168.123.100 y el número del puerto de escucha TCP es 4001, el usuario puede conectarse al puerto como se muestra a continuación. telnet 192.168.123.100 4001

Protocolo
Seleccione “Telnet”, “SSH”, o “Raw TCP” como protocolo. Si los usuarios están utilizando un programa de cliente telnet, seleccione "Telnet". Si los usuarios están utilizando un programa de cliente SSH, seleccione "SSH". Cuando se selecciona "Raw TCP", la comunicación con el socket TCP está disponible directamente entre el servidor de consola y el host remoto.

Tiempo límite de inactividad
Active esta característica para evitar que un cliente se mantenga a la espera en una conexión TCP cuando no haya actividad en un puerto serie durante un periodo de tiempo largo.Si el "Tiempo límite de inactividad" está activado y no hay actividad de datos entre el servidor de consola y el cliente SSH/telnet durante el intervalo de tiempo límite de inactividad especificado (p. ej. cuando no hay actividad de datos a través de un puerto serie), la sesión TCP existente se cerrará automáticamente. Si quiere mantener la conexión indefinidamente, configure el periodo de tiempo límite de inactividad en "0".

TCP Keep-Alive (No se requiere configuración)
Con el fin de evitar que se cierre el acceso a la conexión TCP, el servidor de consola seguirá comprobando el estado de conexión entre el cliente telnet/SSH y el servidor de consola, enviando periódicamente paquetes “keep alive”. Si el cliente telnet/SSH no responde a los paquetes, el sistema considerará la conexión nula. Entonces, el servidor de consola cerrará la conexión telnet/SSH existente, sin tener en cuenta el tiempo de inactividad. Esto evitará que la conexión TCP se bloquee cuando una aplicación se cierra de forma inadecuada o si el vínculo con la red se interrumpe.

Modo de servidor de terminal
En el modo de servidor de terminal, el puerto serie del servidor de consola se configura para esperar datos del dispositivo conectado al puerto. Si se detectan datos, el servidor de consola iniciará una sesión TCP como cliente telnet o SSH en un servidor predefinido. Los usuarios deben definir el servidor antes de que el puerto se configure para un cliente telnet o SSH. Este modo puede utilizarse para acceder a los servidores de la red desde un terminal serie. El Raw TCP también es compatible con el modo de servidor de termina.

```
Terminal server mode (ssh), press any key ...
login:root
passwd:
login as:jeffrey
The authenticity of host '192.168.123.164 (192.168.123.164)' can't be establishe
d.
  RSA key fingerprint is 1c:92:81:af:9f:a7:b5:1f:7c:ab:dc:d9:b7:46:f1:ef.
                                                                        Are you
 sure you want to continue connecting (yes/no)? yes
jeffrey@192.168.123.164's password:
[jeffrey@Jeffrey_Linux jeffrey]$ ls
lincvs-1.3.1-2-RedHat-9.0-i386-bin.rpm  proj                       tmp
lincvs-1.4.3                            qt-x11-free-3.3.3          util
lincvs-1.4.3-0-generic-src.tar          qt-x11-free-3.3.3.tar.bz2
[jeffrey@Jeffrey_Linux jeffrey]$          ← Ctrl-Z / Ctrl-X / Ctrl-C
Terminal server mode (ssh), press any key ...
```

Con el fin de terminar una sesión telnet/SSH/Raw TCP en el modo de servidor de terminal, puede utilizar estas tres secuencias de teclas: (Ctrl-Z / Ctrl-X / Ctrl-C).

Modo de conexión para módem

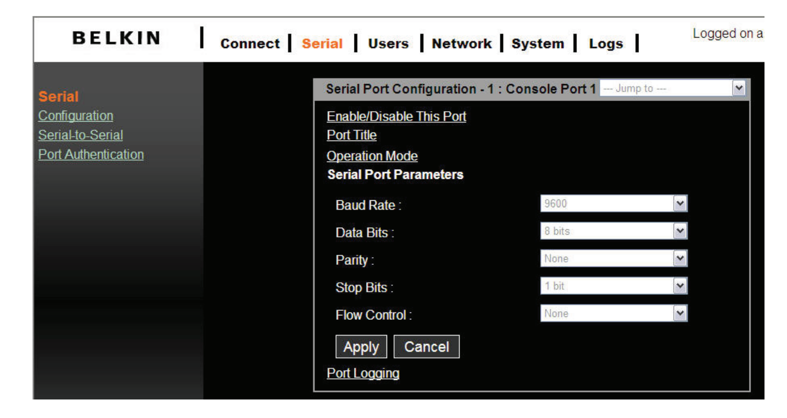
En este modo, el servidor de consola considera que se ha conectado un módem al puerto serie y espera una conexión de una ubicación remota. Cuando un usuario se conecta utilizando una aplicación de terminal, el servidor de consola acepta la conexión y muestra una ventana o un menú apropiado para el usuario que se ha conectado.

Función serie-serie

Por favor, consulte la sección "Función serie-serie" de la página 34 para obtener detalles sobre este modo.

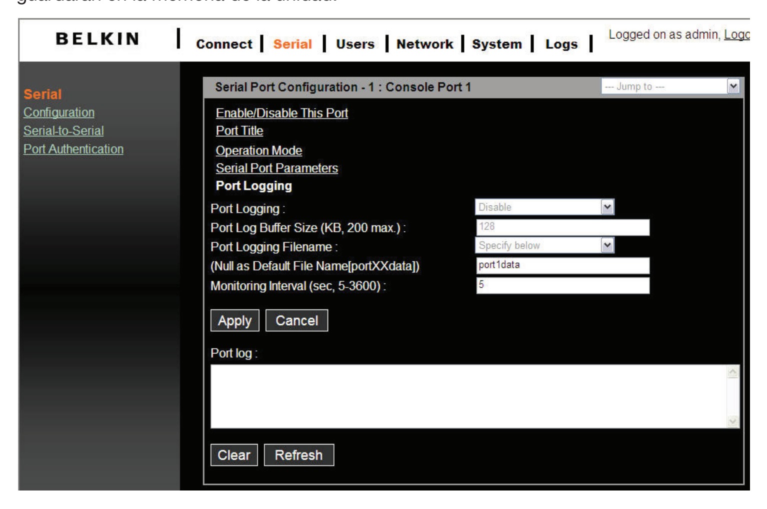
Parámetros del puerto serie

Para conectar el dispositivo serie al puerto serie del servidor de consola, los parámetros del puerto serie de la consola deben coincidir exactamente con los requisitos del dispositivo conectado.



Acceso al puerto

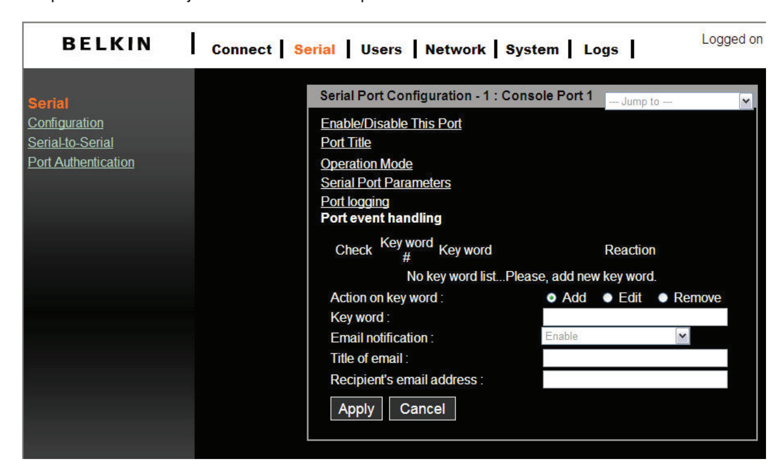
En el modo de servidor de consola, los datos recibidos por el puerto serie de rastreo se guardarán en la memoria de la unidad.



La característica de "Acceso al puerto" es válida y visible sólo si el modo de funcionamiento del puerto serie está configurado en el modo de servidor de consola.

Si la opción "Acceso al puerto" está activada, el usuario puede dejar que el servidor de consola busque una palabra clave definida de los datos de acceso al puerto y envíe un corre electrónico a un administrador mediante las configuraciones "Manejo de los eventos de puerto". Cada respuesta puede configurarse individualmente sobre cada palabra clave. La respuesta puede enviarse por correo electrónico.

Clique sobre "Manejo de los eventos de puerto".



El tamaño de la memoria intermedia para el acceso es de 192 K por puerto. Si los datos de acceso aumentas más que el tamaño de la memoria, los nuevos datos sobrescribirán a los antiguos.

Función pausa

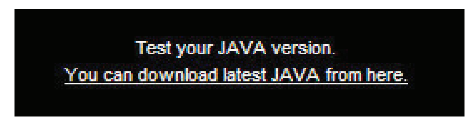
En el modo de servidor de consola, el servidor de consola puede enviar un señal de "pausa" a un dispositivo serie conectado. Una pausa se utiliza a veces para reiniciar la comunicación o para cambiar de modo de funcionamiento del hardware de comunicación, como por ejemplo un módem. Algunos dispositivos de destino, como un servidor Sun™ Solaris™, requieren un carácter nulo (pausa) para generar un mensaje "Aceptar". El efecto de "enviar una pausa mediante un puerto serie" es equivalente a emitir un “STOP-A” en un teclado Sun. Con el fin de enviar una pausa a un dispositivo serie, configúrelo en el modo de servidor de consola y utilice el protocolo Raw TCP o telnet. Clique sobre "Aplicar" para enviar una señal de pausa al puerto serie designado y después al ordenador o servidor conectado.

Conexión

El servidor de consola proporciona un acceso basado en Internet para un dispositivo serie de destino sin necesidad de un programa de cliente telnet separado. Esto se realiza mediante un Applet de Java.

Se utiliza un Applet de Java para proporcionar la interfaz de usuario basada en texto para acceder al puerto serie. El Applet de Java sólo es compatible con el modo de servidor de consola. El usuario no puede acceder al puerto serie mediante Internet cuando está configurado el modo host del puerto con una conexión Raw TCP. Se pedirá un nombre de usuario y una contraseña para acceder al puerto. Una vez autentificado, el usuario tendrá acceso al puerto serie.

Utilice el hipervínculo que se encuentra en la parte de abajo de la página de conexión para comprobar su compatibilidad con Java. O utilice este vínculo para descargar la última versión de Java.

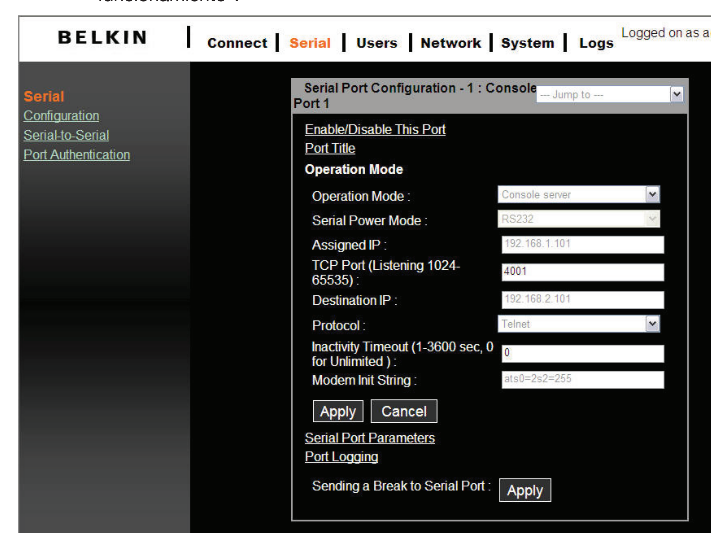


Asegúrese de que activa la opción de compatibilidad con Java de su explorador de Internet y compruebe también la versión del entorno de ejecución Java. Necesitará la versión 1.6.0. o superior si también necesita el servicio de seguridad HTTP (HTTPS).

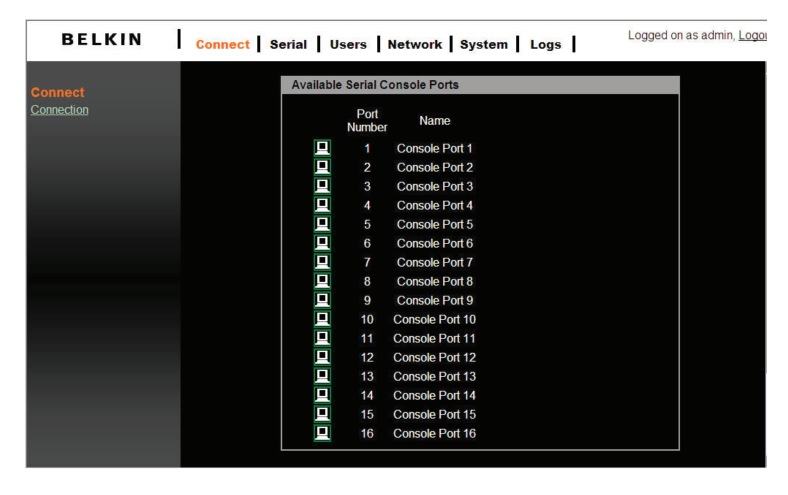
Nota:
- Con el fin de ejecutar esta función el sistema requiere la instalación de JRE versión 6.0 o superior. Puede conseguir el software Java en http://www.java.com/en/download/.

Telnet Java Applet

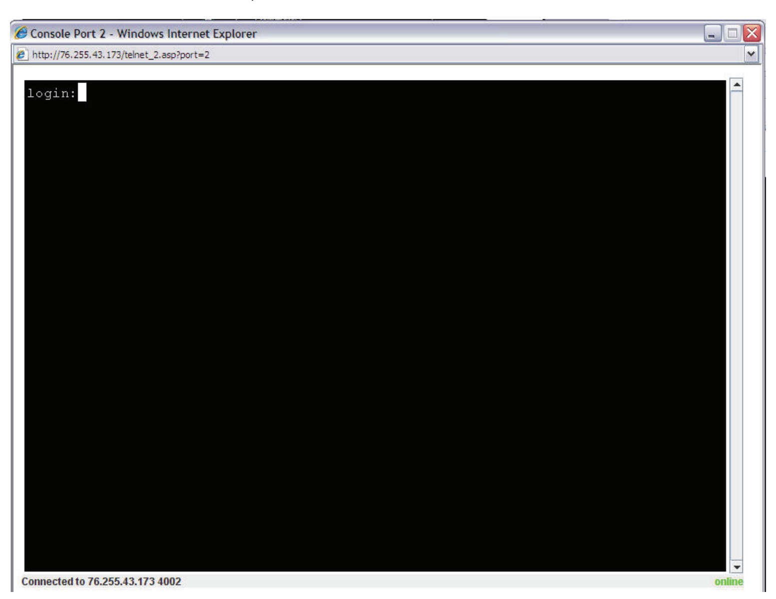
1. Seleccione el protocolo telnet en “Serie > Configuración > Modo de funcionamiento”.



Seleccione "Conectar" en el menú superior y haga click sobre el icono del terminal en la parte izquierda. La aplicación de emulación de terminal abrirá una nueva ventana y le pedirá inicie sesión. Si ve una ventana en blanco, compruebe la compatibilidad de su sistema con la versión de Java.



2. Introduzca el nombre de usuario y la contraseña para iniciar sesión y podrá empezar a utilizarlo como si se tratara de un programa de cliente telnet (p. ej., Telnet DOS, PuTTY).



Nota: El nombre del puerto serie activo aparecerá en la barra de la ventana. Un indicador del estado de la conexión aparecerá también en la parte inferior derecha de la ventana.

Función serie-serie

La función serie-serie le permite utilizar un simple dispositivo terminal (pantalla de vídeo y teclado) para acceder y controlar los dispositivos conectados al servidor de consola, del puerto 1 al 15. Puede también utilizar un convertidor de terminal externo, como el F1D084Eea de Belkin, para conectar su servidor de consola a un conmutador KVM y consolidar el control.

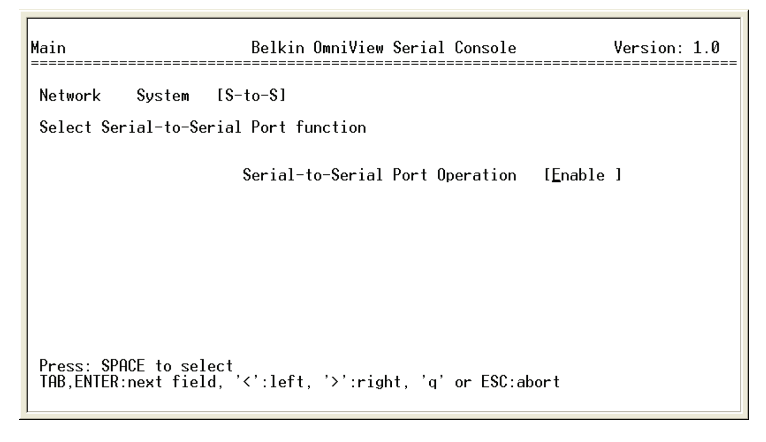
Instalación

Para instalarlo, conecte su dispositivo terminal al puerto 16 del servidor de consola. Esto le permitirá acceder a un dispositivo serie conectado sólo a los puertos del 1 al 15.

Activar y configurar serie-serie

Para configurar la función serie-serie:

1. Active el modo VT-100 de la consola (ver la sección " Asignar una IP desde el puerto VT-100 de la consola (Console, Telnet, SSH)” para obtener detalles) para visualizar la ventana siguiente.
2. Vaya al elemento del menú de dos niveles [S-a-S] “Funcionamiento serie-serie”, y pulse la barra ESPACIADORA para seleccionar “ACTIVAR”. Confirme el cambio para que el sistema se reinicie automáticamente.



3. Ahora desconecte la consola local y vuelva a empezar una nueva sesión de terminal conectándolo al puerto 16.
4. Tras el reinicio (que durará más o menos un minuto) aparecerá la pantalla de la página siguiente. Configure cada ajuste de configuración. Introduzca el valor del "tiempo límite de inactividad" y pulse la barra ESPACIADORA para seleccionar los ajustes de los otros elementos.

Nota:

- Con el fin de mostrar la pantalla de configuración serie a serie siguiente, deberá activar la función serie a serie. La tasa de baudios por defecto está fijada a 9600 8N1 (no reconfigurable) para conseguir la máxima compatibilidad con dispositivos de gestión de terminal de terceras partes.

```
                         Belkin OmniView Serial Console          Version: 1.0
================================================================================
[S-to-S]

 Serial-to-Serial Configuration

                        Connect to Port#     [_2]
                        Inactivity Timeout   [0          ]
                        Baud Rate            [9600  ]
                        Data Bits            [8 bits]
                        Parity               [None]
                        Stop Bits            [1 bit ]
                        Flow Control         [None    ]

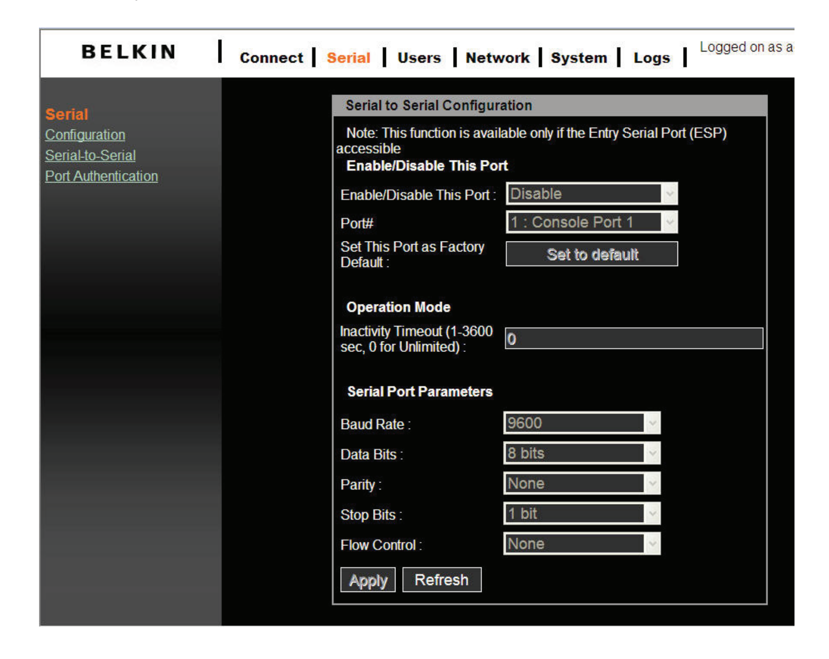
 Press: SPACE to select
 TAB,ENTER:next field, '<':left, '>':right, 'q' or ESC:abort
```

5. Escoja el número de puerto al que desea conectar y aparecerá la ventana siguiente.

```
Serial-to-Serial mode , press any key ...
login:admin
password:
```

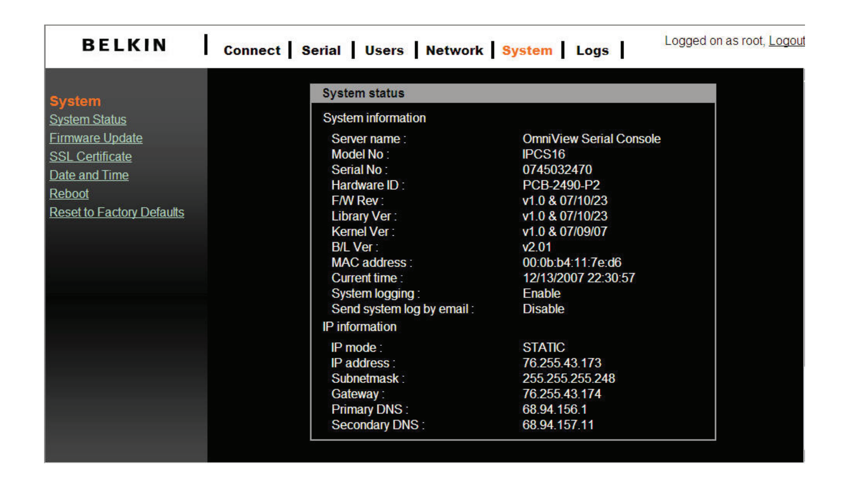
6. Introduzca el nombre de usuario y la contraseña. La conexión del canal de datos entre el puerto 16 y el puerto serie seleccionado se establecerá, de esta manera el administrador puede controlar el dispositivo serie o el servidor.
7. Pulse las teclas “Ctrl” y “C” para salir de la función serie-serie y volver a la pantalla principal de la consola.

La página de Internet también da ajustes de sólo lectura de la función serie-serie, cambiará automáticamente de acuerdo con el cambio de ajuate del VT-100. Haga click sobre "Cancelar" para actualizar los valores.



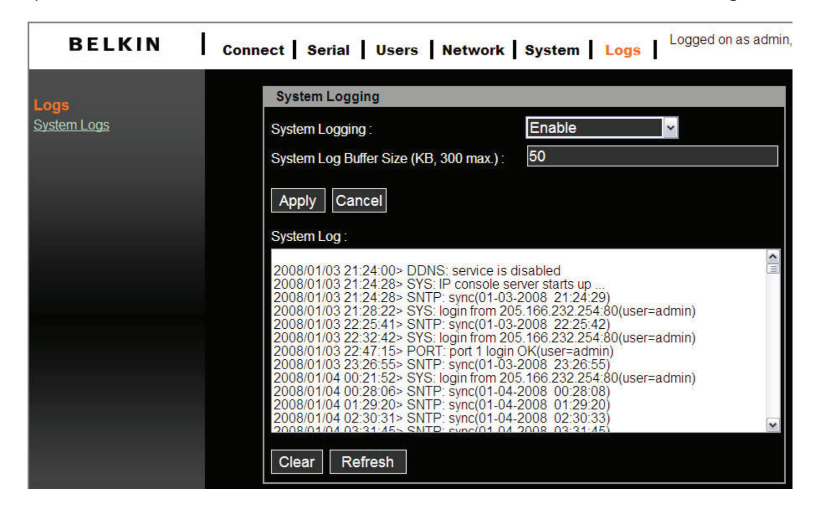
Estado del sistema

La página del "estado de sistema" muestra una lista de información sobre el sistema, como el nombre, el número de serie, las versiones del firmware, la dirección MAC, la hora y los ajustes de red. Los datos de esta página no pueden modificarse. Esta página se actualiza automáticamente cada 10 segundos.



Acceso al sistema

Puede activar o desactivar el proceso de acceso al sistema y ajustar el tamaño de la memoria de acceso. El valor por defecto de la memoria de acceso al sistema es de 50 Kb y se puede incrementar hasta 300 kb como máximo. Si los datos de acceso aumentan más que el tamaño de la memoria establecido, los nuevos datos sobrescribirán a los antiguos.



Los siguientes eventos de sistema han accedido cíclicamente al almacenamiento volátil:

i) SYS (inicio del sistema, tiempo límite de inactividad, autenticación de la cuenta de acceso)

ii) SNTP (tiempo de sincronización de la red)

iii) LOG (borrar el acceso a los eventos del sistema)

iv) PORT (autenticación de acceso al puerto serie)

v) DDNS (evento de registro de dirección IP dinámica)

Administración de usuarios

Al iniciarse, el sistema pedirá al usuario que introduzca su nombre de usuario y su contraseña para acceder al sistema. El administrador puede añadir o eliminar un usuario fácilmente mediante las páginas de Internet.
Hay dos niveles de privilegio de acceso:

Nombre de usuario	Contraseña predeterminada	Privilegios de acceso
admin	admin	Acceso completo
(definición de usuario)	(definición de usuario)	Puede acceder solamente a "Puerto serie" y a "Estado del sistema"

Una página de "Acceso denegado" aparecerá si el usuario no está autorizado a acceder a la página de Internet.

Añadir usuario

Para añadir un usuario:

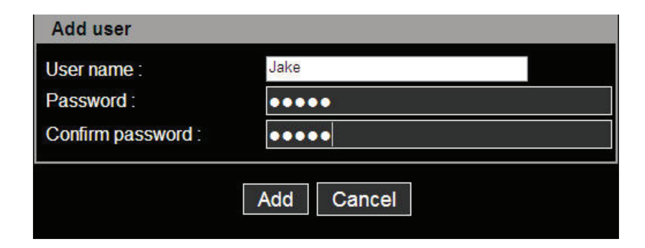
- Compruebe los usuarios en la pantalla de "Administración de usuarios".
- Haga clic en el botón “Añadir”.
- Introduzca el nuevo nombre de usuario y la contraseña.

Directrices del nombre del usuario y la contraseña

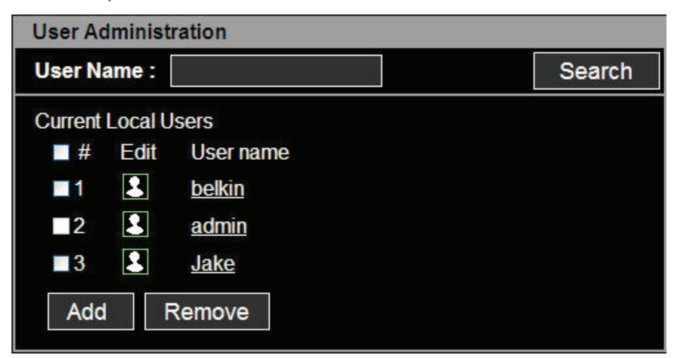
- El primer carácter del nombre de usuario debe ser una letra del alfabeto.
- La contraseña tiene que tener tres caracteres como mínimo.
- El nombre de usuario y la contraseña no deben tener más de 32 caracteres.
- Sólo el usuario “admin” puede acceder a la "Red" y a la "Administración del sistema".



La figura siguiente muestra la pantalla "Añadir usuario".



El nuevo usuario aparecerá en la lista "Nombres de usuario".



Eliminar usuario

Para eliminar un usuario:

- Compruebe los usuarios en la pantalla de "Administración de usuarios".
- Haga clic en el botón "Eliminar".



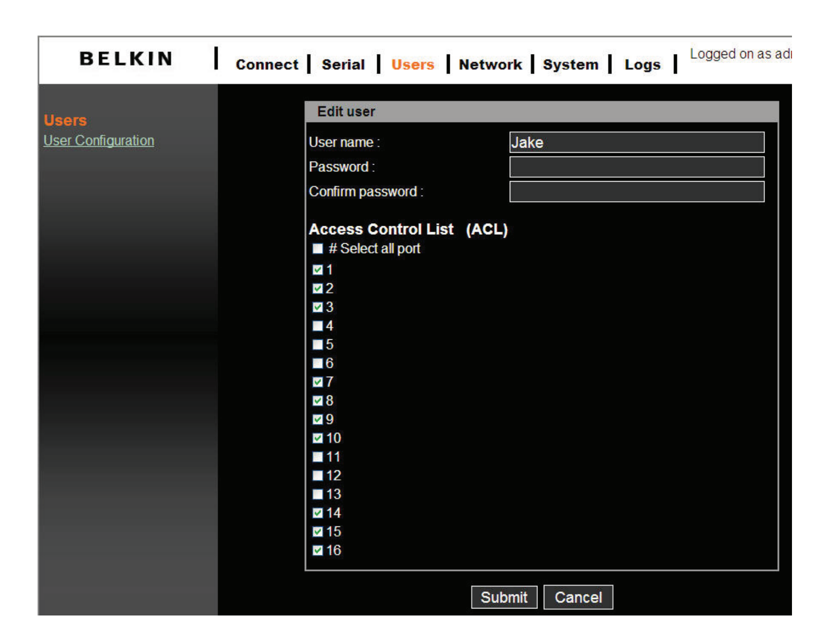
Editar la lista de control de acceso (ACL)

El servidor de consola proporciona la seguridad ACL (Lista de control de acceso), con la que puede especificar el acceso de los usuarios a cada puerto, en lugar de a todos los puertos.

Para editar la ACL.

- Compruebe los usuarios en la pantalla de "Administración de usuarios".
- Haga clic en el icono “Editar”.
- Introduzca el nombre de usuario y la contraseña.
- Seleccione el puerto al que quiere acceder.
- Haga clic en el botón “Enviar”.

Una vez que se haya configurado la ACL de cuentas de usuario, los usuarios podrán acceder o modificar la configuración a los puertos serie a los que estén autorizados. Los usuarios no podrán ver ni configurar los puertos serie a los que no están autorizados.



Cambiar la contraseña

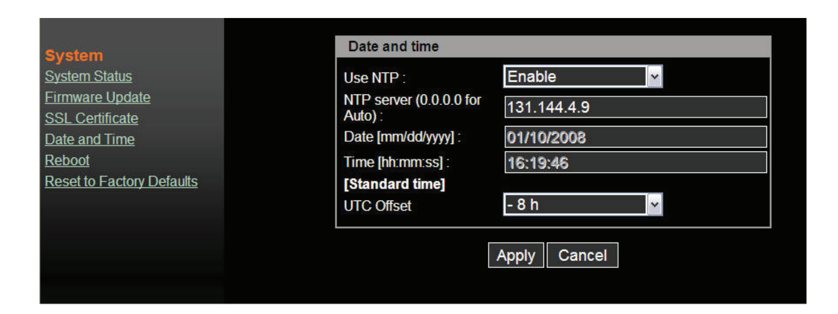
Para cambiar los parámetros de la cuenta de usuario, abra la pantalla "Editar usuario" seleccionando el nombre de usuario en la pantalla "Configuración del usuario" y después edite los parámetros de la cuenta de usuario como si añadiera un usuario.

Fecha y hora (NTP)

El servidor de consola mantiene la información de hora y fecha actual. Una batería interna apoya los ajustes de reloj y calendario. El usuario puede cambiar la fecha y la hora.

Hay dos opciones para ajustar la hora y la fecha. La primera opción es permitir al servidor NTP que mantenga los ajustes de hora y fecha. Si la característica NTP está activada, el servidor de consola obtendrá los datos y la información horaria del servidor NTP en cada reinicio y se alineará automáticamente con el servidor NTP cada hora. Si el servidor NTP está configurado en 0.0.0.0., el servidor de consola utilizará automáticamente los servidores NTP por defecto. En este caso, debería estar conectado de la red a Internet. El segundo método es configurar la fecha y la hora manualmente, sin utilizar el servidor NTP. Es este caso, la información de fecha y hora se mantiene mediante la batería interna.

Convencionalmente, los científicos utilizan una zona horaria, Greenwich Mean Time (GMT). Esta hora también se conoce como Hora Universal (UTC). Puede ajustar la diferencia de zona horaria y fecha con la UTC dependiendo de la ubicación del usuario para configurar la fecha y la hora exactas, y la diferencia horaria con la UTC. El valor "X" de la diferencia puede ser un número entero positivo o negativo. Por favor, consulte la página de Internet http://time_zone.tripod.com/ para ver la diferencia horaria con la UTC.



Nota:

- El servidor de consola ofrece la función RTC (reloj a tiempo real) con una batería de litio (CR2032, 3 V). De esta manera la fecha y la hora se mantendrán activos aunque haya un corte en la alimentación.
- Si pierde repetidamente la información de fecha y hora, por favor sustituya la batería.
- Sustituya la batería CR2032 de 3 voltios por otra igual o del mismo tipo que le recomiende el fabricante de la misma. Una batería puede explotar si no se instala correctamente. Deshágase de las baterías según las instrucciones del fabricante.

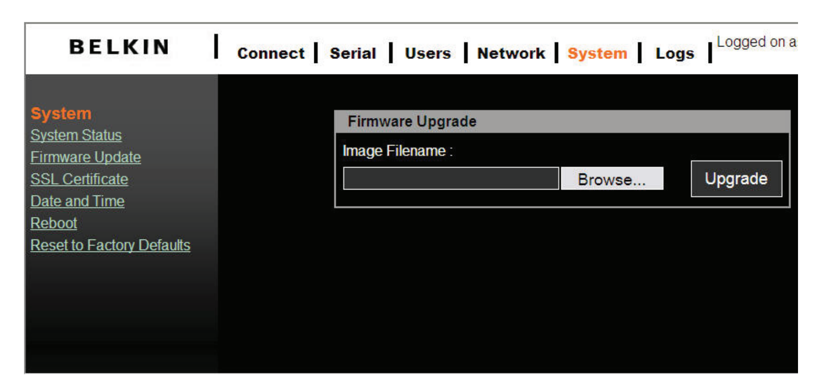
Actualización del firmware

El firmware puede actualizarse fácilmente mediante Internet. Esta sección describe el proceso de actualización.

La última versión del software está disponible en www.belkin.com/support.

Actualización desde la interfaz de Internet

Véase la página "Sistema > Actualización del software".

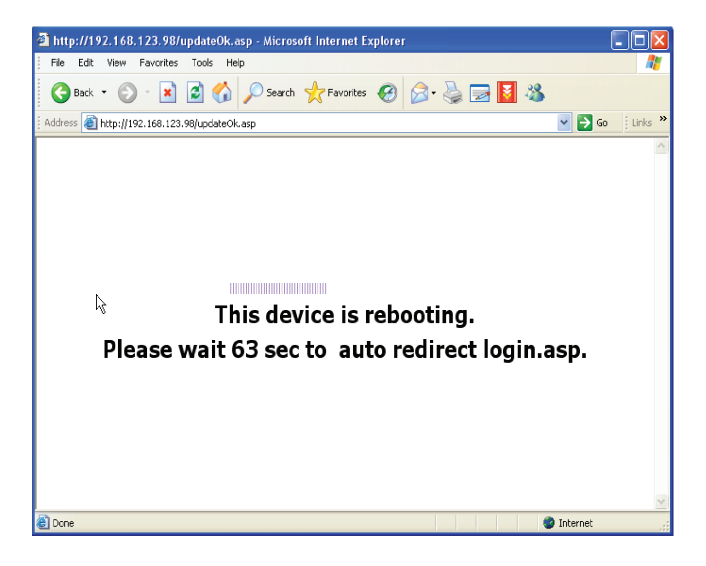


Clique sobre "Examinar" para buscar el archivo del firmware en la ventana del explorador. Navegue por su PC y seleccione el archivo del firmware. Clique sobre "abrir" para confirmar su selección.

Cuando haya seleccionado el archivo del firmware apropiado, haga click sobre "Actualizar" para iniciar el proceso de actualización del firmware. La interfaz de Internet mostrará la barra de progreso de transferencia del archivo. Al mismo tiempo, el puerto LED del panel frontal parpadeará en series para indicar que el proceso de actualización está en proceso.

¡Atención! NO desconecte la alimentación ni el cable Ethernet durante el proceso de actualización. Si lo hace puede provocar un fallo en la actualización del software y destruir la imagen de la memoria.

El servidor de consola se reiniciará automáticamente cuando se haya completado el proceso de actualización para activar el nuevo firmware. Cuando el contador termine, el explorador le enviará a la página de acceso. Puede referirse a la página "Estado de sistema" para comprobar la versión del firmware y confirmar la actualización.

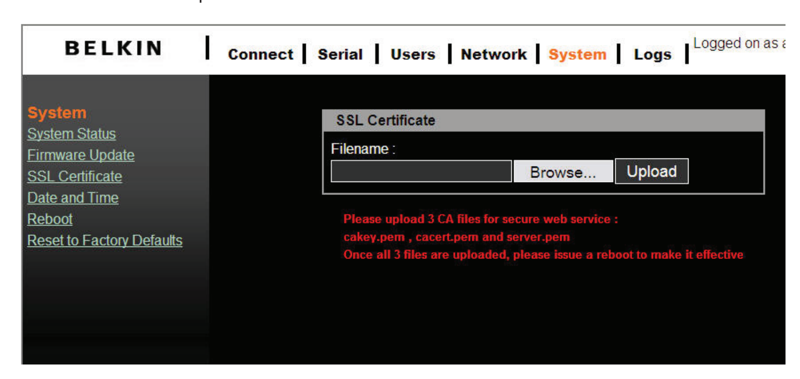


Certificado SSL

Un certificado SSL es una identificación digital que contiene información para atestiguar que el certificado pertenece a una persona, una organización, un servidor o a otra entidad en concreto especificada en el certificado. El servidor de consola soporta la seguridad HTTP (aka https) para realizar cambios de configuración mediante Internet. El certificado SSl del servidor identifica el servidor de consola para que pueda confiar en el certificado y realizar los cambios de configuración de forma confidencial.

El servidor de consola es capaz de cargar los archivos del certificado personalizado del servidor de Internet. El conjunto de archivos del certificado está compuesto por tres archivos (cacert.pem, cakey.pem, y server.pem). Los tres archivos certificados se cargarán para completar la actualización del certificado. La interfaz de carga de archivos es similar a la de la actualización del firmware.

Una vez que se haya cargado todos los archivos del certificado, los usuarios deberán reiniciar manualmente para hacer efectivo el nuevo certificado.



Examine los archivos CA preparados (siga el procedimiento del anexo E para preparar correctamente los tres archivos CA con los mismos nombres de archivo asignados), y cárguelos en el servidor de consola. Por favor, compruebe cada archivo antes de cargarlo. Un conjunto de archivos CA falso puede desactivar la función de seguridad HTTP.

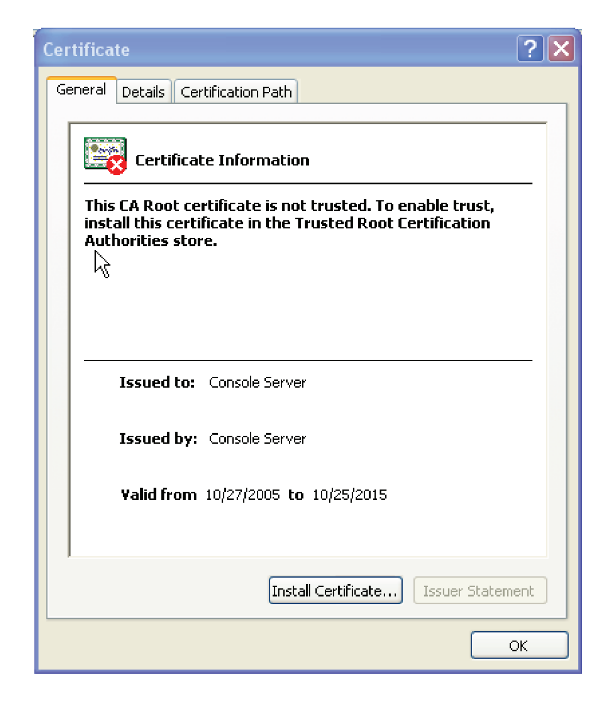
Nota:

- Si los archivos CA se dañan, los usuarios pueden recuperar los ajustes de fábrica mediante "System > Reset to Factory Defaults" (Sistema > Reiniciar con los ajustes por defecto).. Se recuperarán os antiguos archivos CA.
- Como la longitud de la ubicación de los archivos CA está limitada (256 caracteres), le recomendamos que ponga todos sur archivos en "C:\upgrade" para administrarlos

Certificado de seguridad HTTP

La conexión https del explorador abrirá un servicio de Internet seguro para el servidor de consola (puerto de servicio 443). El explorador le mostrará un mensaje de seguridad para notificarle el certificado. Deberá aceptar el certificado para empezar el servicio de Internet seguro. Los usuarios pueden escoger "Ver el certificado" y justificar si el servidor de Internet conectado es de confianza.

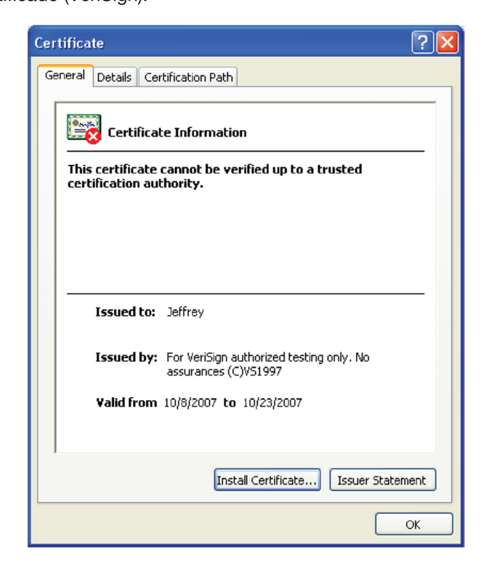

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

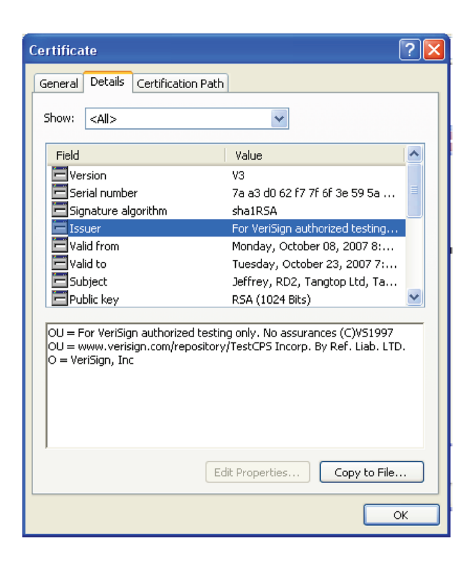

Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Console Server
Issued by: Console Server
Valid from 10/27/2005 to 10/25/2015
Install Certificate...
Issuer Statement
OK

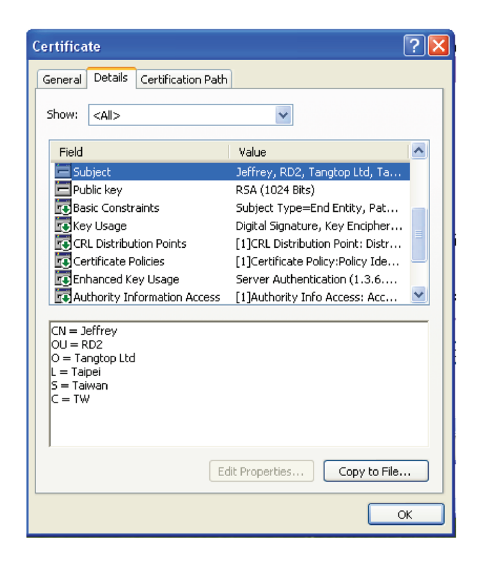
Otra forma de diferenciar una conexión a Internet segura de una no segura es buscar el símbolo de un candado en el navegador (esquina inferior derecha del navegador Internet Explorer). ^Puede hacer doble click sobre el símbolo para examinar la información detallada del certificado del servidor.

Una vez haya preparado un conjunto de archivos CA firmados públicamente, cárguelos desde la página "Certificado SSL". Se pedirá que reinicie el sistema para que surja efecto.

El ejemplo siguiente muestra un certificado firmado públicamente e información registrada a la autoridad del certificado (VeriSign).

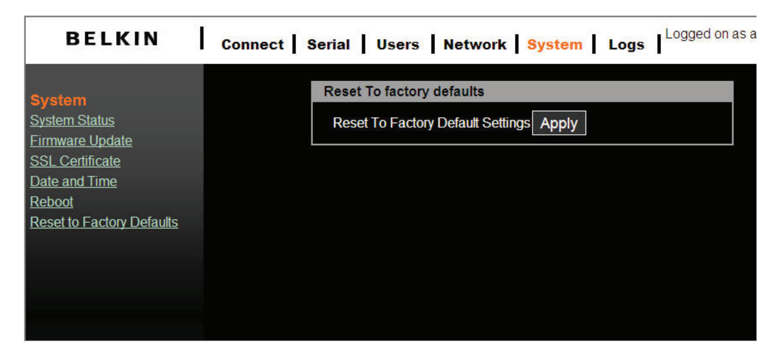



Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Version
V3
Serial number
7a a3 d0 62 f7 7f 6f 3e 59 5a ...
Signature algorithm
sha1RSA
Issuer
For VeriSign authorized testing...
Valid from
Monday, October 08, 2007 8:...
Valid to
Tuesday, October 23, 2007 7:...
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
OU = For VeriSign authorized testing only. No assurances (C)VS1997
OU = www.verisign.com/repository/TestCPS Incorp. By Ref. Liab. LTD.
O = VeriSign, Inc
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
Jeffrey, RD2, Tangtop Ltd, Ta...
Public key
RSA (1024 Bits)
Basic Constraints
Subject Type=End Entity, Pat...
Key Usage
Digital Signature, Key Encipher...
CRL Distribution Points
[1]CRL Distribution Point: Distr...
Certificate Policies
[1]Certificate Policy:Policy Ide...
Enhanced Key Usage
Server Authentication (1.3.6....
Authority Information Access
[1]Authority Info Access: Acc...
CN = Jeffrey
OU = RD2
O = Tangtop Ltd
L = Taipei
S = Taiwan
C = TW
Edit Properties...
Copy to File...
OK

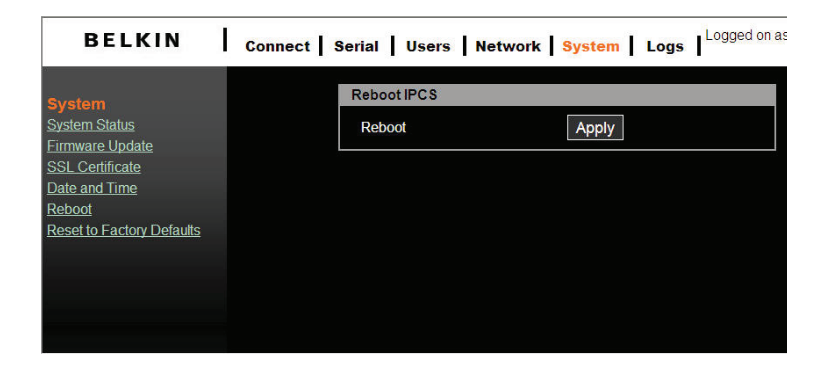
Restablecimiento de los ajustes de fábrica predeterminados

Para volver a los ajustes de fábrica predeterminados, haga click sobre "Aplicar".



Reiniciar

Puede activar el servidor de consola para realizar un reinicio a través de la red. el reinicio es obligatorio cuando se ha completado la carga del certificado CA.



Ajustes por defecto

Nombre del servidor **DHCP** **Dirección IP** **Máscara de red** **Puerta de enlace**	BelkinSC Activado 192.168.2.156 255.255.255.0 192.168.2.1
Número de serie: **Dirección MAC**	xxxxxxxxx (impreso en la base de la unidad) xx:xx:xx:xx (impreso en la base de la unidad)
Versión y fecha	Número de versión y fecha actual del firmware
Nombre de usuario **Contraseña**	admin admin
Protocolo (serie) **Protocolo (Internet)** **Filtro IP**	Telnet HTTP Desactivar
Puertos serie: **Velocidad de transmisión en baudios** **Datos/Parar** **Paridad** **Control del flujo** **Tiempo límite del puerto serie** **Modo de funcionamiento** **Puerto TCP**	 9600 8-1 Ninguno Ninguno 0 segundos Servidor de consola **Puerto 1:** 4001 **Puerto 2:** 4002 - - - - - - - - **Puerto 16:** 4016

F1D120ea (RJ45F – DB9F DTE)

Adaptador de DB9 hembra a DTE

Aplicaciones Bay Accelar, Nortel, etc.
Nº del artículo: F1D120ea - Un sólo paquete
F1D120ea8PK (Pack de 8)

Adaptador		
Señal	RJ45	DB9F
DSR	1	4
DCD	6	
RTS	2	8
GND	3	5
TxD	4	2
RxD	5	3
CTS	7	7
DTR	8	6 1 (DCD)

F1D121ea (RJ45F – DB25F DTE)

Adaptador de DB25 hembra a DTE

Aplicaciones Dispositivos DTE como PCs
Nº del artículo: F1D120ea - Un sólo paquete

Adaptador		
Señal	RJ45	DB25F
DSR	1	20
DCD	6	
RTS	2	5
GND	3	7
TxD	4	3
RxD	5	2
CTS	7	4
DTR	8	6
		8 (DCD)

F1D122ea (RJ45F – DB25M DCE)

Adaptador de DB25 macho a DCE

Aplicaciones Módems
Nº del artículo: F1D122ea - Un sólo paquete

Adaptador		
Señal	RJ45	DB25M
DSR	1	6
RTS	2	4
GND	3	5
TxD	4	2
RxD	5	3
DCD	6	1
CTS	7	5
DTR	8	20

F1D123ea (RJ45F – DB25M DTE)

Adaptador de DB25 macho a DTE

Aplicaciones Sun SPARC, etc.
Nº del artículo: F1D123ea - Un sólo paquete

<table>
<tr><th colspan="3">Adaptador</th></tr>
<tr><td>Señal</td><td>RJ45</td><td>DB25M</td></tr>
<tr><td>DSR</td><td>1</td><td rowspan="2">20</td></tr>
<tr><td>DCD</td><td>6</td></tr>
<tr><td>RTS</td><td>2</td><td>5</td></tr>
<tr><td>GND</td><td>3</td><td>7</td></tr>
<tr><td>TxD</td><td>4</td><td>3</td></tr>
<tr><td>RxD</td><td>5</td><td>2</td></tr>
<tr><td>CTS</td><td>7</td><td>4</td></tr>
<tr><td>DTR</td><td>8</td><td>6</td></tr>
</table>

F1D124ea (RJ45F – RJ45M CISCO)

Adaptador macho RJ45

Aplicaciones Dispositivos Sun
Nº del artículo: F1D124ea - Un sólo paquete
F1D124ea8PK (Pack de 8)

Adaptador		
Señal	RJ45	RJ45M
DSR	1	2
RTS	2	8
GND	3	4
		5
TxD	4	6
RxD	5	3
CTS	7	1
DTR	8	7

Cable RJ45 con conectores Ethernet estándar

Pin	Descripción
1	Tx+
2	Tx-
3	Rx+
4	NC
5	NC
6	Rx-
7	NC
8	NC

Los números de puerto se dividen en tres gamas: Puertos conocidos, puertos registrados y puertos dinámicos y/o privados. Los puertos conocidos son del 0 al 1023. Los puertos registrados son del 1024 al 49151. Los puertos dinámicos y7o privados son del 49152 al 65535.

Los puertos conocidos los asigna IANA y, en la mayoría de sistemas, sólo pueden utilizarse mediante procesos de sistema o mediante programas ejecutados por usuarios privilegiados. La tabla siguiente muestra algunos de los números de puerto conocidos. Para obtener más detalles, por favor visite la página de Internet de IANA: http://www.iana.org/assignments/port-numbers.

Número de puerto	Protocolo	TCP/UDP
21	FTP (File Transfer Protocol, protocolo de transferencia de archivos)	TCP
22	SSH, Secure Shell	TCP
23	Telnet	TCP
25	SMTP, Simple Mail Transfer Protocolos (Protocolo simple de transferencia de correo)	TCP
37	Hora	TCP, UDP
39	RLP (Resource Location Protocol, protocolo de localización de recursos)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	Servidor BOOTP	UDP
68	Cliente BOOTP	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol, protocolo de transferencia de datos de red)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

BOOTP, Bootstrap Protocolos (Protocolo bootstrap o de autoarranque)
Similar al DHCP pero para redes más pequeñas. Asigna la dirección IP automáticamente para una duración determinada.

CHAP, Challenge Handshake Authentication Protocolos (o protocolo de reto-respuesta)
Un protocolo seguro para conectarse a un sistema, es más seguro que el PAP.

DHCP, Dynamic Host Configuration Protocolos (Protocolo de configuración de host dinámico)
Protocolo de Internet para automatizar la configuración de los ordenadores que utilizan TCP/IP.

DNS, Domain Name Server (Servidor de nombres de dominio)
Un sistema que permite a un servidor de nombres de red traducir los nombres de host en direcciones IP numéricas.

Kerberos
Un protocolo de autenticación de red que proporciona una autenticación fuerte para aplicaciones de cliente/servidor utilizando criptografía de clave secreta.

LDAP, Lightweight Directory Access Protocol (Protocolo de acceso a directorios ligeros)
Un protocolo para acceder a la información del directorio.

NAT, Network Address Translation (traducción de direcciones de red)
Un estándar de Internet que activa una LAN para utilizar un conjunto de direcciones IP para tráfico interno y un segundo conjunto de direcciones para el tráfico externo. Esto permite a una empresa proteger sus datos internos del Internet público.

NFS, Network File System (Sistema de archivos de red)
Un protocolo que permite compartir archivos en una red. Los usuarios pueden ver, almacenar y actualizar archivos en un ordenador remoto. Puede utilizar NFS para montar todo o parte de un sistema de archivos. Los usuarios pueden acceder a la parte montada con el mismo privilegio que tienen de acceso a los archivos.

NIS, Network Information System (Sistema de información de red)
Sistema desarrollado por Sun Microsystems para distribuir datos de sistema como usuarios y nombres de host entre ordenadores en una red.

NMS Network Management System (Sistema de gestión de red)
El NMS actúa como un servidor central, pidiendo y recibiendo información tipo SNMP desde cualquier ordenador que utilice SNMP.

NTP, Network Time Protocolos (Protocolo de hora de red)
Un protocolo utilizado para sincronizar la hora en ordenadores en red y equipos.

PAP, Password Authentication Protocolos (Protocolo de autenticación por contraseña)
Un método de autenticación de usuario en el que el nombre de usuario y la contraseña se transmiten mediante una red y se comparan con una lista aparejada de nombres y contraseñas.

PPP Point-to-Point Protocolos (Protocolo de punto a punto)
Un protocolo para crear y ejecutar IP y otros protocolos de red mediante un vínculo serie.

RADIUS, Remote Authentication Dial-In User Service (Remote Dial de autenticación de usuario de servicios)
Un protocolo de autenticación y contabilidad. Activa el acceso remoto a los servidores para comunicarse con un servidor central y autentificar a los usuarios que se conecten y sus permisos de acceso. Una empresa almacena los perfiles de usuario en una base de datos central que los servidores remotos pueden compartir.

SNMP, Simple Network Management Protocolos (Protocolo simple de gestión de red):
Un protocolo que utilizan los administradores de sistemas para supervisar las redes y los dispositivos conectados y para responder a las peticiones de otros hosts de la red.

SMTP, Simple Mail Transfer Protocolos (Protocolo simple de transferencia de correo)
Protocolo TCP/IP para enviar correos electrónicos entre servidores

SSL, Secure Socket Layer (Capa de conexión segura)
Un protocolo que proporciona servicios de autenticación y encriptación entre un servidor de Internet y un navegador de Internet.

SSH, Secure Shell
Un protocolo de transporte seguro basado en criptografía de claves públicas.

TACACS+, Terminal Access Controller Access Control System (Sistema de control de acceso mediante control del acceso desde terminales)
Un método de autenticación utilizado en redes UNIX. Permite a un servidor de acceso remoto que se comunique con un servidor de autenticación para determinar si el usuario tiene acceso a la red.

Telnet
Un protocolo de terminal que proporciona un método fácil para crear conexiones de terminal con un host de red.

El servidor de consola soporta la configuración de páginas de Internet seguras (aka https). hay dos tipos de archivos certificados para la autenticación del servidor.

- Autofirmado: Los usuarios pueden crear los archivos del certificado ellos mismos. El inconveniente es que al cliente, se le pedirá que acepte un certificado firmado por una autoridad no conocida por el navegador. Normalmente el navegador del cliente debería aceptar el certificado sólo una vez y no se le pedirá más adelante.
- Firmado por una autoridad de certificación: Los usuarios crean los archivos CA y los envían a la autoridad de certificación para que lo firmen. La principal ventaja es que al cliente no se le pedirá que acepte un certificado.

Los usuarios deberán instalar las herramientas de OpenSSL antes de crear los archivos CA antes mencionados. Aquí le explicamos cómo generar un certificado para el servidor de Internet del servidor de consola utilizando OpenSSL y la shell de Linux. Puede descargar las herramientas OpenSSL de: http://www.openssl.org/.

1. CA autofirmado:

i) Crear una clave y un certificado X.509:

cuando el comando de Linux se lo solicite:

openssl req -x509 -newkey rsa:1024 -days 1024 -keyout cakey.pem -out cacert.pem

Las opciones que`pueden cambiarse son:

* el algoritmo PK puede cambiarse de rsa a dsa y también la longitud de la clave en bits (512, 1024, 2048, 4096).

* el periodo de validez del certificado se configura para 1024 días, menos de tres años.

También puede configurar una fecha de inicio y de fin de validez del certificado. se le pedirá que introduzca la frase de paso PEM dos veces para la clave y después deberá introducir cierta información necesaria para el certificado:

Aquí tiene un ejemplo:

Nombre del país	<EE.UU.>
Nombre del estado o de la provincia	<Su estado>
Ciudad o localidad	<Anchorage>
Nombre de la organización	<u negocio>
Unidad Organizacional Prolix	<R y D>
Nombre común (NOMBRE DEL HOST DEL SERVIDOR)	<IPCS>
Dirección de correo electrónico del administrador de servicios	<you@yourdomain.com>

ii) Frase de paso:

openssl rsa -in cakey.pem -out cakey-nopassword.pem

iii) Combina la clave y los archivos del certificado X.509 en el servidor PEM:

cat cakey-nopassword.pem cacert.pem > server.pem

iv) Recoge los tres archivos PEM y los prepara para cargarlos en el servidor IPCS:

server.pem , cacert.pem , cakey.pem

2. Firmado con CA de confianza:

i) Prepara la clave privada **cakey.pem:**

openssl genrsa –des3 –out cakey.pem 1024

significado de los parámetros:

genrsa : genera una clave privada RSA

des3 : encripta el certificado mediante DES3

1024 : el tamaño de la clave es de 1024-bit

ii) Preparar una petición de certificado firmado:

openssl req –new –key cakey.pem –out server.csr

las herramientas de OpenSSL mostrarán al usuario un mensaje para guiarle al completar el formulario de registro. Una vez completado, los usuarios pueden enviar el archivo CSR a www.verisign.com para probarlo o remitirse a http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp (en Taiwán) para pedir un certificado firmado. Consiga el certificado y nombre el archivo como “cacert.pem”.

iii) Frase de paso:

openssl rsa –in cakey.pem –out cakey-nopassword.pem

iv) Combina la clave y los archivos del certificado X.509 en el servidor PEM:

cat cakey-nopassword.pem cacert.pem > server.pem

v) Recoja los tres archivos PEM para cargarlos.:

server.pem , cacert.pem , cakey.pem

Declaración de la FCC

DECLARACIÓN DE CONFORMIDAD CON LAS NORMATIVAS DE LA FCC SOBRE COMPATIBILIDAD ELECTROMAGNÉTICA

Nosotros, Belkin International, Inc., con sede en 501 West Walnut Street, Compton, CA 90220 (EE.UU.), declaramos bajo nuestra sola responsabilidad que el producto: F1DP116S, al que hace referencia la presente declaración:

Cumple con la sección 15 de las normativas de la FCC. Su utilización está sujeta a las siguientes dos condiciones:

(1) este dispositivo no debe provocar interferencias nocivas y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado.

Las pruebas realizadas con este equipo dan como resultado el cumplimiento con los límites establecidos para un dispositivo digital de la clase A, de acuerdo a la sección 15 de las normativas de la FCC. Estos límites se han establecido con el fin de proporcionar una protección suficiente contra interferencias nocivas en zonas comerciales. Este equipo genera, emplea y puede irradiar energía de radiofrecuencias y, si no se instala y se emplea según las instrucciones del manual, puede causar interferencias nocivas en las comunicaciones por radioemisión. El funcionamiento de este equipo en una zona residencial probablemente causará interferencias, en cuyo caso se puede solicitar al usuario que tome las medidas oportunas para evitar las interferencias, y deberá hacerse cargo de los gastos.

Le présent appareil numérique n’émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le Ministére des Communications du Canada.

Declaración de conformidad CE

Nosotros, Belkin International Inc., declaramos bajo nuestra sola responsabilidad que el producto F1DP116S, al que hace referencia la presente declaración, está en conformidad con el Estándar de Emisiones EN55022 Clase A, el Estándar de Inmunidad EN55024 y LVD EN61000-3-2 y EN61000-3-3.

ICES

Este aparato digital de la clase A cumple con la norma canadiense ICES-003.

Garantía del producto de 2 años de Belkin International, Inc.

La cobertura de la presente garantía.

Belkin International, Inc. (“Belkin”) otorga una garantía al comprador original según la cual el producto Belkin no tendrá defectos en cuanto a diseño, montaje, materiales o mano de obra.

Cuál es el período de cobertura.

Belkin garantiza el producto Belkin durante dos años.

¿Cómo resolveremos los problemas?
Garantía del producto.
Belkin reparará o sustituirá, según decida, cualquier producto defectuoso sin ningún tipo de cargo (excepto los gastos de envío del producto).

¿Qué excluye la presente garantía?
Todas las garantías mencionadas anteriormente resultarán nulas y sin valor alguno si el producto Belkin no se le proporciona a Belkin para su inspección bajo requerimiento de Belkin con cargo al comprador únicamente o si Belkin determina que el producto Belkin se ha instalado de un modo inadecuado, alterado de algún modo o forzado. La garantía del producto de Belkin no lo protege de los desastres naturales tales como inundaciones, terremotos, rayos, vandalismo, robos, mal uso, erosión, agotamiento, desuso o daño a causa de interrupciones en la alimentación (p. ej. apagones) modificación o alteración no autorizadas de programas o sistemas.

Para obtener asistencia.
Para obtener asistencia sobre algún producto de Belkin, debe seguir los siguientes pasos:

1. Póngase en contacto con Belkin International, Inc en 501 W. Walnut St., Compton CA 90220, a la atención de: Servicio de atención al cliente, o llame al teléfono (800)-223-5546, en un plazo de 15 días desde el momento de la incidencia. Tenga preparada la siguiente información:
   a. El número de artículo del producto Belkin.
   b. El lugar de compra del producto.
   c. Cuándo compró el producto.
   d. Copia de la factura original.

2. El servicio de atención al cliente de Belkin le informará sobre cómo enviar la factura y el producto Belkin y sobre cómo proceder con su reclamación.

Belkin se reserva el derecho de revisar el producto Belkin dañado. Todos los gastos de envío del producto Belkin a Belkin para su inspección correrán a cargo del comprador exclusivamente. Si Belkin determina, según su propio criterio, que resulta poco práctico el envío de los equipos averiados a Belkin, Belkin podrá designar, según su propio criterio, una empresa de reparación de equipos para que inspeccione y estime el coste de la reparación de dichos equipos. Los gastos, si existen, de envío del equipo a dicha empresa de reparaciones, y de su valoración, correrán exclusivamente a cargo del comprador. El equipo dañado deberá permanecer disponible para su inspección hasta que haya finalizado la reclamación. Si se solucionan las reclamaciones por negociación, Belkin se reserva el derecho a subrogar la garantía por cualquier póliza de seguros del comprador.

Relación de la garantía con la legislación estatal.
ESTA GARANTÍA CONTIENE LA GARANTÍA EXCLUSIVA DE BELKIN. NO EXISTEN OTRAS GARANTÍAS EXPLÍCITAS O IMPLÍCITAS, EXCEPTO LAS ESTABLECIDAS POR LEY, INCLUYENDO LA GARANTÍA IMPLÍCITA O LAS CONDICIONES DE CALIDAD, APTITUD PARA LA VENTA O PARA CUALQUIER PROPÓSITO EN CONCRETO Y, TALES GARANTÍAS IMPLÍCITAS, SI ES QUE EXISTE ALGUNA, ESTÁN LIMITADAS A LA DURACIÓN DE ESTA GARANTÍA.

Ciertas jurisdicciones no permiten la limitación de duración de las garantías implícitas, por lo que puede que las anteriores limitaciones no le afecten.

EN NINGÚN CASO BELKIN SERÁ RESPONSABLE DE LOS DAÑOS IMPREVISTOS, ESPECIALES, DIRECTOS, INDIRECTOS, CONSECUENTES O MÚLTIPLES, INCLUYENDO ENTRE OTROS LA PÉRDIDA DE NEGOCIO O BENEFICIOS QUE PUEDA SURGIR DE LA VENTA O EL EMPLEO DE CUALQUIER PRODUCTO BELKIN, INCLUSO SI BELKIN HA SIDO INFORMADA DE LA POSIBILIDAD DE DICHOS DAÑOS.

Esta garantía le proporciona derechos legales específicos y también podría beneficiarse de otros derechos que pueden variar entre las distintas jurisdicciones. Algunas jurisdicciones no permiten la exclusión o limitación de los daños fortuitos, consecuentes, o de otro tipo, por lo que puede que las limitaciones mencionadas anteriormente no le afecten.

BELKIN®

Servidor de consola serie OmniView®

Asistencia técnica gratuita*

Podrá encontrar más información en nuestra página web www.belkin.com a través del servicio de asistencia técnica. Si desea ponerse en contacto con el servicio de asistencia técnica por teléfono, le rogamos que llame al número correspondiente de la siguiente lista*.

*Se aplican tarifas locales

País	Número	Dirección de Internet
AUSTRIA	0820 200766	http://www.belkin.com/uk/support/
BÉLGICA	07 07 00 073	http://www.belkin.com/nl/support/
REPÚBLICA CHECA	239 000 406	http://www.belkin.com/uk/support/
DINAMARCA	701 22 403	http://www.belkin.com/uk/support/
FINLANDIA	00800 - 22 35 54 60	http://www.belkin.com/uk/support/
FRANCIA	08 - 25 54 00 26	http://www.belkin.com/fr/support/
ALEMANIA	0180 - 500 57 09	http://www.belkin.com/de/support/
GRECIA	00800 - 44 14 23 90	http://www.belkin.com/uk/support/
HUNGRÍA	06 - 17 77 49 06	http://www.belkin.com/uk/support/
ISLANDIA	800 8534	http://www.belkin.com/uk/support/
IRLANDA	0818 55 50 06	http://www.belkin.com/uk/support/
ITALIA	02 - 69 43 02 51	http://www.belkin.com/it/ support
LUXEMBURGO	34 20 80 85 60	http://www.belkin.com/uk/support/
PAÍSES BAJOS	0900 - 040 07 90 0,10€ por minuto	http://www.belkin.com/nl/support/
NORUEGA	81 50 0287	http://www.belkin.com/uk/support/
POLONIA	00800 - 441 17 37	http://www.belkin.com/uk/support/
PORTUGAL	707 200 676	http://www.belkin.com/uk/support/
RUSIA	495 580 9541	http://www.belkin.com/uk/support/
SUDÁFRICA	0800 - 99 15 21	http://www.belkin.com/uk/support/
ESPAÑA	902 - 02 43 66	http://www.belkin.com/es/support/
SUECIA	07 - 71 40 04 53	http://www.belkin.com/uk/support/
SUIZA	08 - 48 00 02 19	http://www.belkin.com/uk/support/
REINO UNIDO	0845 - 607 77 87	http://www.belkin.com/uk/support/
OTROS PAÍSES	+44 - 1933 35 20 00	

BELKIN®

www.belkin.com

Belkin Ltd.
Express Business Park
Shipton Way, Rushden
NN10 6GL (Reino Unido)

Belkin B.V.
Boeing Avenue 333
1119 PH Schiphol-Rijk
Países Bajos

Belkin GmbH
Hanebergstrasse 2
80637 Munich
Alemania

Belkin SAS
130 rue de Silly
92100 Boulogne-Billancourt
Francia

Belkin Iberia
Avda. Cerro del Águila 3
28700 San Sebastián de los Reyes
España

Belkin Sweden
Knarrarnäsgatan 7
164 40 Kista
Suecia

 P75598ea